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

Review of CSE's Network-based solutions and related Cybersecurity & Information Assurance activities

NSIRA // Review 2021 - 17

SECRET // CEO // SOLICITOR-CLIENT

Table of Contents

List of Acronyms

ALPR – Acknowledgement of Legal and Policy Requirements

CBS – Cloud-based solutions

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

CERT – Computer Emergency Response Team

CSIA – Cybersecurity and information assurance (aspect of CSE's mandate; section 17 of the *CSE Act*)

CSE – Communications Security Establishment

CSE Act – *Communications Security Establishment Act*

[redacted]

GC – Government of Canada

GII – Global Information Infrastructure

HBS – Host-based solutions

[redacted]

IOC – Indicator of compromise

IRTC – Information relating to a Canadian or a person in Canada

MND – Minister of National Defence

MoU – Memorandum of Understanding

MPS – Mission Policy Suite (CSE)

NBS – Network-based solutions

NDA – *National Defence Act* (CSE's lawful authority prior to the *CSE Act*)

OCSEC – Office of the CSE Commissioner (1996-2019)

NSICOP – National Security and Intelligence Committee of Parliamentarians

PAI – Publicly available information; see glossary.

PC – Private communication; see glossary.

PCO – Privy Council Office

RCP – Releasable cybersecurity product

REP – Reasonable expectation of privacy (of a Canadian or person in Canada)

RFI – Request for Information

SIGINT – Signals Intelligence

SME – Subject-Matter Expert

SOI – System of Importance (as designated by the Minister in s. 21(1) of the *CSE Act*)

SSC – Shared Services Canada

Glossary of Terms

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

Incidentally. As per section 23(5) of the *CSE Act*: "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."

Minister. In this report, 'Minister' refers to the Minister of National Defence.

Private Communication (PC). As per section 183 of the *Criminal Code*. Any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it.

Publicly available information (PAI). As per section 2 of the *CSE Act*; PAI means "information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase. It does not include information in respect of which a Canadian or person in Canada has a reasonable expectation of privacy."

Reasonable Expectation of Privacy (REP) of a Canadian or person in Canada. Section 8 of the Charter of Rights and Freedoms provides that everyone has the right to be secure against an unreasonable search or seizure. A search for the purposes of section 8 is any state activity that interferes with a "reasonable expectation of privacy" (REP). As noted above, information in respect of which a Canadian or person in Canada has a REP is excluded from the definition of PAI in the *CSE Act*. CSE Act ss. 22(3) and 22(4) prohibit certain activities that interfere with the REP of a Canadian or person in Canada furthering the Foreign Intelligence and Cybersecurity and Information Assurance aspects of their mandate unless authorized by the Minister as set out in the *Act*.

Solution. In this report, "solution" refers to a system combining hardware and/or software that allows it to monitor for and respond to cyber threats. This can include a broad range of specific capabilities.

System owner. In this report, "system owner" refers to a Government of Canada department or agency, or a component of it, that perform duties related to the management or protection of computer systems, sometimes including the systems of other departments or agencies. In the case of CSE's NBS cybersecurity program, [redacted] departments or agencies are "partners" of CSE in the context of implementing its NBS cybersecurity program ("NBS partners"). NBS partners are system owners for various Internet-connected networks; some of the partners further offer these NBS-protected networking services to other departments or agencies. The [redacted] NBS partners are SSC, [redacted] and CSE itself.

System user. In this report, "system user" refers to an individual user of a computer system or network.

I. EXECUTIVE SUMMARY

1. The Government of Canada views cybersecurity as one of the most serious economic and national security challenges facing Canada and Canadians. The coming into force of the *Communications Security Establishment Act* (CSE Act) in 2019 introduced significant changes to CSE's authorities, including to CSE's cybersecurity and information assurance (CSIA) activities. While the acquisition and analysis of vast amounts of information is critically important to identifying and preventing cybersecurity threats, CSIA activities are often intrusive and engage important personal privacy interests.

2. This is NSIRA's first review of CSE's CSIA activities. In addition to CSE, NSIRA incorporated Shared Services Canada (SSC) into this review, given its role as a system owner for a large portion of Government of Canada networks. This is the first time NSIRA has reviewed SSC.

3. The review initially centred on one of three primary cybersecurity solutions used by CSE to detect and prevent threats against the digital information and information infrastructures it protects: network-based solutions (NBS). In doing so, the review mapped the lifecycle of cybersecurity information as it is initially captured by the NBS sensors, and is subsequently processed through the various systems that comprise CSE's cyber defence ecosystem.

4. Overall, NSIRA found that CSE operates a comprehensive and integrated ecosystem of cybersecurity systems, tools, and capabilities to protect against cyber threats, with a design that incorporates measures meant to protect the privacy of Canadians and persons in Canada.

5. NSIRA also analysed two main thematic areas: transparency, and privacy. NSIRA made findings and recommendations regarding the transparency of some of CSE's information provided, and commitments made, to the Minister of National Defence in its applications for Ministerial authorizations for CSE's cybersecurity activities on federal infrastructure.

6. NSIRA also examined a specific case pertaining to a cybersecurity information acquisition activity by CSE from an external source that may have implicated a reasonable expectation of privacy of Canadians or persons in Canada. CSE continued this activity after the Intelligence Commissioner determined he could not approve the activity as proposed in the corresponding Ministerial authorization. NSIRA made findings and recommendations about how CSE addressed this issue, which resulted from an incongruence in the CSE Act that restricts the ability for an authorization to be issued for this specific acquisition activity under the CSIA aspect of CSE's mandate.

7. While CSE only partially met NSIRA's expectations for responsiveness on this review, NSIRA was able to independently verify CSE information provided during the review.

II. INTRODUCTION

8. The Communications Security Establishment (CSE), and the Canadian Centre for Cyber Security (CCCS, or Cyber Centre) within it, protect electronic information and information systems of Canadian federal institutions, and other systems of importance to the Government of Canada (GC). Prior to NSIRA's creation in 2019, the Office of the CSE Commissioner (OCSEC) conducted annual reviews of CSE cyber defence activities; the most recent such review was completed in early 2019.[1]

9. The *Communications Security Establishment Act* (CSE Act) introduced significant changes to CSE's authorities, including in the context of the cybersecurity and information assurance aspect of its mandate (henceforth: cybersecurity aspect, or CSIA aspect).[2] This is NSIRA's first review of CSIA activities carried out by CSE, and the Cyber Centre therein. The review aimed to understand details of CSIA activities.

10. CSE uses a variety of tools, tradecraft, and services in the fulfillment of the CSIA aspect of its mandate. Prominent within CSE's cybersecurity activities are its use of three complementary cybersecurity solutions:[3] network-based solutions (NBS), host-based solutions (HBS), and cloud-based solutions (CBS). Information from these three solutions, alongside other information, feeds CSE intrusion detection and intrusion prevention systems. In turn, these systems enable CSE to protect the electronic information and information infrastructures of federal institutions and systems of importance to the GC.

Authority

11. This review was conducted pursuant to paragraphs 8(1)(a) and 8(1)(b) of the *National Security and Intelligence Review Agency Act*.[4]

Scope of Review

12. Given the use of NBS across government networks since 2006,[5] NSIRA initially chose to focus the review on this solution specifically.[6] However, as NSIRA learned more about CSE's cybersecurity activities, systems, and techniques, it became clear that the initial scope was too narrow. For example, as described to the Minister by the Chief of CSE in her 2019-2020 application for Cybersecurity Activities on Federal Infrastructure, all three of CSE's solutions are supported by three main activities: Dynamic Defence, analysis, and retention of information.[7] NSIRA determined that while NBS provides a unique source of threat information into CSE's cyber defence ecosystem, it was more appropriate to examine NBS in the context of CSE's broader CSIA activities. Ultimately, this

[1] Office of the Communications Security Establishment Commissioner, *Annual Review of the Communications Security Establishment's Cyber Defence Activities under the 2017-2018 Cyber Defence Activities Ministerial Authorization*. File no. 2200-127. This review found that CSE complied with the law, and made no recommendations.
[2] *Communications Security Establishment Act*, SC 2019, c 13, s 76 [CSE Act]. See section 17.
[3] "Solution" is CSE's term for a system combining hardware and/or software that allows it to monitor for and respond to cyber threats. This can include a broad range of specific capabilities.
[4] *National Security and Intelligence Review Agency Act,* SC 2019, c 13, s 2.
[5] For details including a timeline of cyber defence sensor development, see: NSICOP, "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack.", August 11, 2021. Available online at: https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-en.html, page 87.
[6] NSIRA Public Annual Report 2021, page 28, available online at: https://nsira-ossnr.gc.ca/wp-content/uploads/Annual-Report-2021-PDF.pdf.
[7] CSE, Application for CSE cybersecurity activities on federal infrastructures 2019-2020, sections IX-XI.

review omits an examination of host-based and cloud-based solutions. However, in its focus on NBS, the review expanded outward to CSIA activities more broadly, so long as these activities were related to NBS. For example, the second part of the Analysis section focuses on a case study pertaining to external sources of data that are used to improve how NBS functions.

13. The report begins with an overview of NBS and related CSE CSIA activities, including applicable legal and policy frameworks. This section makes an overarching finding about NBS and CSIA activities. Next, the Analysis section details more specific findings and recommendations, which focus on the handling of information related to a Canadian or a person in Canada (IRTC), which may be further subject to a reasonable expectation of privacy (REP) of a Canadian or a person in Canada. The analysis comprises two themes:

- Transparency about the nature of information collected by NBS; and
- Acquisition of information from external sources that may contain a REP of a Canadian or person in Canada.

14. Annexes contain relevant contextual or supplementary information. Of note, Annex A describes the process and steps by which information captured by NBS moves through CSE's cyber defence ecosystem, from the initial collection of this information, to the publication or sharing of reports based on analysis of this information. Annex B discusses the use of cybersecurity information across the aspects of CSE's mandate.[8]

Methodology

15. The period under review ranged from August 1, 2019 to June 17, 2021, though NSIRA received information from before and after this timeframe when deemed relevant. Notably, the specific case explored in the 'Reasonable Expectation of Privacy' part of the Analysis section of the report originated from activities that occurred during the period under review, but the specific case itself—and CSE's response to it—occurred entirely *after* June 2021.

16. NSIRA analysed a wide range of information in CSE's possession, including extensive documentation related to: process, legal advice, technical detail, information logs, compliance reporting, and more. This included applications submitted by the Chief of CSE to the Minister for Ministerial Authorization of cybersecurity activities on federal infrastructures. Documents provided to NSIRA included correspondence between CSE and other Government of Canada entities that received, or considered the adoption of, CSE's NBS and related cybersecurity solutions. NSIRA also received seven briefings and/or technical demonstrations from CSE subject-matter experts.

17. Shared Services Canada (SSC) was also scoped into the review given its role as a system owner for a large portion of GC networks. NSIRA analysed documentation from SSC and received one briefing and one technical demonstration from SSC subject-matter experts. In addition to its relevance to some of NSIRA's areas of analysis, SSC information helped to corroborate information NSIRA received from CSE.

18. As per section 13 of the NSIRA Act, NSIRA cooperated with the Secretariat of the National Security and Intelligence Committee of Parliamentarians (NSICOP) to avoid unnecessary duplication of work.[9] In this spirit, the report avoids, whenever possible, repetition of information discussed in the August 2021 NSICOP *Special Report on the Government of Canada's Framework and Activities to*

[8] The *CSE Act* sets out the five aspects of CSE's mandate: foreign intelligence, CSIA, defensive cyber operations, active cyber operations, and technical and operation assistance.
[9] *National Security and Intelligence Review Agency Act,* SC 2019, c 13, s 2.

Defend its Systems and Networks from Cyber Attack.[10]

Review Statements

19. Overall, CSE partially met NSIRA's expectations for responsiveness on this review. While CSE partially met, or did not meet, several of NSIRA's expectations for responsiveness during the first half of the review, CSE's responsiveness met NSIRA's expectations in the second half of the review. Given this was NSIRA's first time incorporating SSC into a review, NSIRA faced initial challenges and delays in engaging SSC on this review. However, once appropriate contacts with SSC were established, SSC met NSIRA's expectations for responsiveness.

20. NSIRA was able to verify information received during the review in a manner that met NSIRA's expectations.

III. OVERVIEW OF NBS AND CSIA ACTIVITIES

Finding no. 1: NSIRA found that CSE operates a comprehensive and integrated ecosystem of cybersecurity systems, tools, and capabilities to protect against cyber threats, with a design that incorporates measures meant to protect the privacy of Canadians and persons in Canada.

What is CSE's CSIA program?

21. The Government of Canada views cybersecurity as "one of the most serious economic and national security challenges" facing Canada and Canadians.[11] As described in CSE's National Cyber Security Threat Assessment 2023-2024, the threat surface available to malicious cyber actors has expanded in recent years, and Canadians and Canadian entities remain vulnerable to cyber threats, most notably cybercrime (including ransomware), and threats from nation-state actors in the context of geopolitical competition.[12]

22. The GC created the Canadian Centre for Cyber Security, within CSE, in October 2018. The Cyber Centre's creation consolidated the roles and responsibilities of CSE's information technology security program, Public Safety Canada's Canadian Cyber Incident Response Centre, and some of the functions of SSC's Security Operations Centre. Today, CSE's CSIA program provides almost all GC entities—as well as applicable systems of importance—a centralized and unified security operations centre running on a comprehensive suite of interconnected tools for analysis and mitigation, both manual and automated. The CSIA program, which benefits from integration with information from CSE's foreign intelligence activities, involves the ingestion and subsequent processing of a massive volume of data from wide-ranging sources to improve threat identification and enable real-time action against threats. Compliance measures, including those meant to protect the privacy of Canadians and persons in Canada, are integrated into the data flow as cyber events are identified, and steps are taken to mitigate or remediate the corresponding threats. Annex A describes the lifecycle of information originating from NBS sensors and processed through CSE's cyber defence ecosystem.

---

[10] See NSICOP, "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," August 11, 2021. Available at: https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-en.html.

[11] CSE, Foreword by the Minister of National Defence, National Cyber Threat Assessment 2020, available at: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020.

[12] Ibid; Message from the Head of the Cyber Centre.

23. The CSIA program also advises government institutions, owners of systems of importance, and the public on cyber threats and cyber defence, through services ranging from published guidance to hands-on analysis and support. NSIRA's review did not examine this component of the CSIA program.

24. In some cases, CSE's CSIA solutions are used by non-GC entities outside of Canada. For example, since 2020, the United Kingdom's National Cyber Security Centre has adopted and used CSE's host-based solutions (HBS) to better secure U.K. government networks.[13] [redacted] Although this review did not assess the efficacy of NBS or CSE's CSIA systems and activities, NSIRA did not observe any information to suggest that they were ineffective. On the contrary, NSIRA saw specific cases where information acquired through NBS was used to respond to malicious cyber activity.

What are CCCS cybersecurity solutions?

25. CSE uses NBS, HBS, and CBS, often referred to as 'sensors', for cyber defence purposes on the information infrastructures of participating federal institutions or applicable systems of importance. CSE's three solutions supplement commercially-available measures for detecting malicious cyber activity, such as anti-virus and firewall software, and are used for two main functions: to identify malicious activity, and defend against it. These solutions, through both manual and automated analysis, identify anomalous behaviour and, if deemed malicious, block the same or similar activities from occurring in the future.

26. Of the three solutions, NBS was the first to be developed, in 2006, and deployed on GC networks beginning in 2009. During the period of review, CSE had deployed NBS only on GC network infrastructure.[14] NBS captures all traffic passing into and out of a given network and sends this information to CSE through a physical 'tap'. As a result, CSE obtains a vast amount of information, including all network traffic, emails, internet browsing information, and more.[15]

27. NBS collects packets and packet data. Packets are the raw building blocks of data sent over networks, including the internet. Files can be reconstructed from packets, allowing CSE to collect emails, browsing history, or anything else transmitted to or from a network monitored by NBS. In contrast to NBS' collection of packets, HBS collects host activity events, and CBS collects logs and content from cloud services.[16] NBS packet collection allows CSE analysts to query for information that appears only in network data, and thus would not appear in HBS or CBS information.

28. There are two forms of capabilities across all three of CSE's cyber defence solutions: passive, and dynamic.[17] Passive capabilities involve sensors designed to detect, analyse, and assist in the identification of cyber threats to GC systems. In the context of NBS, sensors capture network traffic through CSE detection capabilities, regularly informed by data from both classified and unclassified

---

[13] CSE webpage, Host-based sensors, available at: https://cyber.gc.ca/en/news-events/host-based-sensors.
[14] This is in contrast with Host-Based Solutions, which had in some cases also been deployed on systems designated as being of importance to the Government of Canada as per paragraph 21(1) of the *CSE Act*.
[15] On average, as of 2021, CSE collected [redacted] from federal departments per day.
[16] NBS sensors collect [redacted] meaning that [redacted] HBS and CBS do not collect packets.
[17] Passive NBS was formerly known under the codename [redacted]. Dynamic Defence was formerly referred to via the codename [redacted]. Note that passive and dynamic modes are not unique to NBS; as of the period under review, dynamic defence was being implemented for HBS and was being developed for CBS. Passive capabilities existed on all three types of sensors: NBS, HBS, and CBS. In cybersecurity industry terms, passive NBS can be compared to a network intrusion detection system (NIDS), while dynamic NBS can be compared to a network intrusion prevention system (NIPS). The two systems work hand-in-hand.

sources, to identify activity of potential concern. Passive NBS, upon detecting suspicious or anomalous activity, can alert analysts for manual action or trigger automated responses.

29. Dynamic Defence, also referred to as 'mitigation actions', involves automatic action against identified malicious indicators of compromise (IOCs) that pose a threat to GC systems and networks. The automatic action comprising Dynamic Defence includes various measures, for example: detecting and preventing malicious scanning activity;[18] blocking/filtering malicious IP addresses and domains; and detecting and blocking certain kinds of cyberattacks.[19] Dynamic Defence leverages threat information from NBS, HBS, and CBS—as well as from [redacted] open sources, classified sources (e.g.: SIGINT), malware analyses, forensic investigations, and disclosures—to automatically act against malicious cyber activity without the need for intervention by human operators.[20] Furthermore, departments—such as SSC—can request CSE to block certain IOCs.[21] Dynamic Defence leverages techniques of machine learning, a branch of artificial intelligence, including for the recognition of malicious patterns, such as computer-generated domain-names.

30. As Annex A describes in further detail, CSE's CSIA ecosystem collects extensive data, and this data moves through four main steps: collection; analysis; retention and disposal; and reporting and use. The majority of this collected data is designed to be deleted as per internal CSE data retention requirements. To retain data rather than deleting it, CSE considers the relevance, necessity, and essentiality of the data. Data which CSE has determined to retain can be used to inform cyber defences, and can be shared both inside and outside of the GC—often in a way that removes personal information from the data.

31. To deploy NBS onto various GC networks, CSE must establish a partnership with the department or agency that owns the system. During the period of review, CSE had [redacted] partnerships with federal entities for NBS ("NBS partners", the system owners of NBS-protected networks): [redacted] SSC, and CSE itself. Within these [redacted] partnerships, some partners further extend NBS services to other GC departments and agencies whose networks are managed by the partner in question. For example, SSC managed the networks of—and thereby extended CSE NBS services to—approximately 90 GC entities, including [redacted].[22] This means that all inbound and outbound network traffic collected from all of those entities is copied and transmitted to CSE. Of note, during the period of review, all [redacted] of CSE's partners were clients of more sensor solutions or other CSIA services than just NBS.

Figure 1 is a CSE graphic that depicts CSE's [redacted] NBS partners, including itself.[23]

[18] Threat actors frequently scan targeted networks for vulnerabilities (e.g., outdated software or inadvertently exposed information). If detected, these scans can be prevented or mitigated.
[19] The examples provided above were referred to with the codenames: [redacted] respectively.
[20] CSE Application for CSE cybersecurity activities on federal infrastructures 2019-2020, paragraph 54.
[21] SSC "often" requests CSE to block certain IoCs.
[22] 78 departments or agencies consumed SSC's Enterprise Internet Service (EIS) as of August 2022; all 78 were receiving NBS protection. In addition, NSIRA understands that some of these departments or agencies within the SSC umbrella offered, in turn, networking services to other GC entities.
[23] For an explanation of these departmental abbreviations, see: https://www.canada.ca/en/government/dept.html.

32. As mentioned above, CSE acquires, uses, and analyses cybersecurity information from the global information infrastructure (GII) in addition to, and in order to enhance, the information originating from the tripartite solutions (HBS, NBS, CBS).[24] The acquisition and use of sources of information other than from these three solutions is discussed in the Analysis section of this report (section IV).

Legal basis for cybersecurity and information assurance (CSIA) activities

33. The CSE Act provides authority for CSE to conduct CSIA activities, and this aspect of the mandate is described in section 17 of the *Act*. Importantly, the CSE Act places constraints on CSIA activities; they cannot be directed at a Canadian or at any person in Canada and must not infringe the *Charter of Rights and Freedoms*.[25]

34. CSIA activities, by their nature, are often intrusive and engage personal privacy interests. The CSE Act provides that the Minister may authorize CSIA activities that would otherwise be prohibited by subsection 22(4) of the *Act*. These include activities that may contravene Acts of Parliament or that would involve the acquisition by CSE of information from the GII that interferes with a REP of a Canadian or person in Canada. In order to issue an authorization, the Minister must conclude that there are reasonable grounds to believe that any activity that would be authorized by it is reasonable and proportionate,[26] in addition to four stipulations outlined in subsection 34(3) of the CSE Act, some of which are discussed throughout this review.[27]

35. The Minister can issue two types of authorization for CSIA activities: for federal infrastructures (27(1)), and for non-federal infrastructures (27(2)). Given that NBS is deployed on GC networks, the CSIA authorizations examined as part of this review were all authorized under 27(1) rather than 27(2). An authorization issued under 27(1) authorizes CSE to "access a federal institution's information infrastructure and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it … from mischief, unauthorized use or disruption."[28]

---

[24] CSE Application for CSE cybersecurity activities on federal infrastructures 2022-2023, paragraph 6.
[25] CSE Act, subsection 22(1).
[26] CSE Act, subsection 34(1): "The Minister may issue an authorization under subsection 26(1), 27(1) or (2), 29(1) or 30(1) only if he or she concludes that there are reasonable grounds to believe that any activity that would be authorized by it is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities."
[27] Paragraphs 34(3)(a), (b), (c), and (d) of the CSE Act refer, respectively, to: retention of information; consent; necessity of information acquisition; and information related to a Canadian or person in Canada (IRTC).
[28] CSE Act, subsection 27(1).

36. In addition, as with authorizations issued under the foreign intelligence aspect of CSE's mandate, CSIA authorizations are valid only once they have been approved by the Intelligence Commissioner.[29]

Policy framework for cybersecurity and information assurance (CSIA) activities

37. CSE's internal policy framework governing activities relating to its CSIA activities is described within the Mission Policy Suite Cybersecurity (MPS Cybersecurity). Although the MPS Cybersecurity does not explicitly mention the NBS program, the document nonetheless provides overarching policy requirements for all CSIA activities, including those carried out under an authorization such as the NBS program.

38. For example, the MPS Cybersecurity sets out the operational policy requirements that apply to information management of data acquired from the NBS program. More specifically, the MPS provides guidance on assessing levels of sensitivity of the information, access rights to information, handling requirements for specific types of information, including assessments and tracking,[30] as well as related retention requirements. The MPS also provides guidelines specific to engagement and information sharing with external entities. This includes engagement prior to deploying a tool or service, as well as relating to the dissemination of information acquired through cybersecurity activities. The MPS Cybersecurity also describes elements of operational compliance in the cybersecurity context.

IV. ANALYSIS

Transparency about the nature of NBS collection

Information related to a Canadian or a person in Canada (IRTC)

Finding no. 2: NSIRA found that CSE treated all network-based solutions (NBS) information as information related to a Canadian or a person in Canada (IRTC), and applied measures intended to protect privacy to all NBS-acquired information.

Finding no. 3: NSIRA found that information acquired through NBS will, by its nature, always include information related to a Canadian or person in Canada (IRTC) and is certain to include some information for which there is a reasonable expectation of privacy (REP) of a Canadian or person in Canada. This was not transparently communicated in corresponding applications to the Minister.

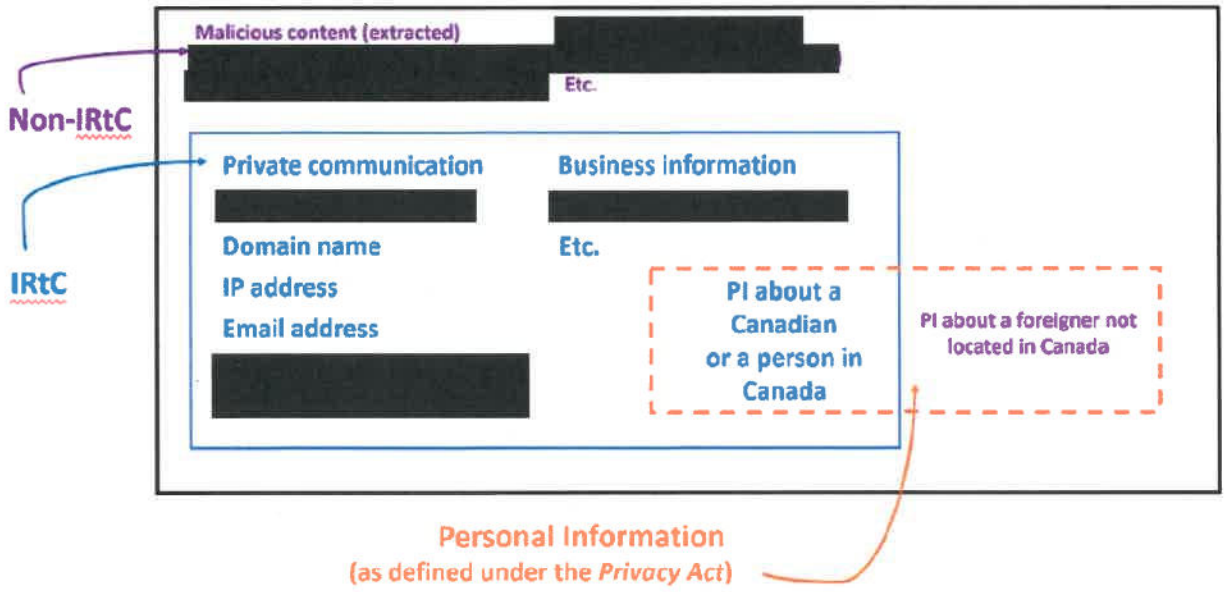
39. While the CSE Act mentions IRTC several times,[31] it does not define it. According to CSE internal policy, IRTC is:

> "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. It can include Canadian identifying information (CII), which is any information that identifies, or could be used to

[29] CSE Act, section 28. The Intelligence Commissioner reviews whether the conclusions made by the Minister in issuing the authorization are reasonable.
[30] Such as: IRTC, publicly-available information, solicitor-client privileged information, and private communications.
[31] 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".

identify, a Canadian or person in Canada, including entities such as corporations and other organizations... IRtC can also include information that will not necessarily lead to the identification of a Canadian or person in Canada..."[32]

Figure 2 (below) is a CSE graphic that depicts examples of information that may or may not be related to a Canadian or a person in Canada in an operational context.[33] Importantly, IRTC can include (but is not limited to) information that would give rise to a REP of a Canadian or person in Canada.



40. CSE is permitted to incidentally acquire IRTC in the course of carrying out activities authorized under a foreign intelligence (ss. 26(1)), cybersecurity (ss. 27(1) or 27(2)), or emergency (s. 40) authorization. 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 differ for CSE's foreign intelligence and CSIA mandate aspects. For the latter, determining "essentiality" means assessing 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 (systems of importance).[34] For foreign intelligence, "essentiality" means an assessment of whether the information is essential to international affairs, defence or security.[35]

---

[32] This definition is found in CSE's internal policy (Mission Policy Suite, MPS) for foreign intelligence activities. An equivalent definition is not available in CSE's internal cybersecurity policy (MPS). NSIRA's Review of Information Sharing Across Aspects of CSE's Mandate (review no. 20-07) also examined IRTC, for example in paragraph 14.
[33] Copied from CSE's internal policy (MPS Cybersecurity, 2022). "PI" refers to personal information.
[34] For cybersecurity, the essentiality requirement is described in 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)."
[35] For foreign intelligence, the essentiality requirement is described in 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."

NBS, IRTC, and information that may interfere with a REP of a Canadian or person in Canada

41. From 2019-2021, CSE produced 1103 releasable cybersecurity products (RCPs) with NBS information that contained IRTC.[36] CSE told NSIRA that it does not share reports beyond the system owner implicated in the report, unless permission is granted by said system owner.[37] As such, each report identifies only one department and removes identities of departments other than the intended recipient.

42. CSE's applications for federal cybersecurity activities, as well as the Minister's corresponding authorizations, state multiple times that HBS, NBS, and CBS are not directed at Canadians or persons in Canada, and that any IRTC that may be acquired through these solutions—including information that may interfere with a REP of a Canadian or person in Canada—is acquired incidentally.[38] CSE, drawing on paragraph 23(3)(a) of the CSE Act, takes the position that "Since the coming into effect of the CSE Act, the conduct of cybersecurity activities on a network for the purposes of helping to defend it is not considered "directed at".[39] This is because the intent and purpose of NBS acquisition is not IRTC, but rather "whether any acquired information indicates a potential cyber incident or cyber threat."[40]

43. In the CSE Chief's 2019-2020 application to the Minister, for cybersecurity activities on federal infrastructure, the Chief notes that "While conducting cybersecurity activities, emails that may contain information relating to Canadian or person in Canada will be incidentally acquired and copied."[41] The corresponding authorization states, in paragraph 2(f)(i) that CSE's acquisition of IRTC in the course of cybersecurity activities is "unavoidable."

44. However, language in all three subsequent annual applications for cybersecurity activities on federal infrastructure—from 2020 to time of writing in May 2023—were considerably more ambiguous about the degree to which IRTC may be acquired by the activities. For example, the applications state on multiple occasions that CSE "may incidentally acquire [IRTC]" or that in the context of the authorization, CSE "may undertake activities that could include the incidental acquisition of [IRTC]."[42]

45. All information collected by NBS is "assumed to contain IRTC". This assumption is based on CSE's position that "Given that NBS data is collected from Canadian infrastructure, it is by nature information related to Canadians." Since 2020, the applications to the Minister for authorization under ss. 27(1) of the CSE Act do not clearly convey the extent of this collection.

---

[36] These RCPs comprised [redacted]

[37] However, during a *later* demonstration, CSE indicated that some information can sometimes be shared beyond the system owner, for example [redacted].

[38] CSE characterizes any acquisition of information that interferes with the REP of a Canadian or person in Canada as 'incidental', and such acquisition does not necessarily mean that this information will be assessed and subsequently processed or used.

[39] Emphasis NSIRA's. NSIRA notes that various OCSEC reviews of CSE cyber defence activities expressed support for this reasoning.

[40] NSIRA notes that this position [redacted]

[41] Application for CSE cybersecurity activities on federal infrastructures 2019-2020, paragraph 109.

[42] Emphasis NSIRA's. See, for example, Application for CSE cybersecurity activities on federal infrastructures: 2020-2021, paragraphs 24, 34, 92, 94; 2021-2022 paragraphs 38, 60, 90, 105; 2022-2023 paragraphs 43, 79, 115, 132.

46. CSE acquires communications *content* through NBS, including the content of emails sent by non-GC email addresses to GC email addresses, and vice-versa. Given the nature of this acquisition, some of the information acquired by CSE is certain to contain information that interferes with the REP of a Canadian or person in Canada. Yet CSE's authorizations and corresponding applications do not fully reflect this reality. Instead, the authorizations include language stating that the acquisition of information "presents a risk that CSE may interfere with the [REP]",[43] and the corresponding application informs the Minister that "CSE runs the risk that it may" acquire information that interferes with a REP when engaged in the described CSIA activities.[44] The corresponding applications include similar conditional language. In reality, NBS is certain to acquire information for which there is a REP for a Canadian or person in Canada.

47. One significant change introduced by the CSE Act is the entrenchment of the concepts of IRTC, and REP. This is a change from the privacy provisions—including "private communication" (PC)—found in CSE's previous statutory home in Part V.1 of the *National Defence Act*.[45] This change reflects the development and increasing sophistication of legal privacy concepts.

48. As per section 24 of the CSE Act, CSE must ensure that measures are in place to protect the privacy of Canadians and persons in Canada in the use, analysis, retention, and disclosure of information; some of these measures are described in Annex A. CSE stated that it is "developing a series of Privacy Impact Assessments that examine the creation, collection, and handling of personal information within the Cyber Security program", though these were not ready during the review period.

49. The fact that NBS collection from Canadian federal infrastructures is, by its nature, certain to include IRTC—including information that interferes with the REP of a Canadian or person in Canada—is neither surprising nor novel. It would not be possible to conduct effective cybersecurity activities of federal institutions' electronic infrastructure and information infrastructures without collecting information in this manner. Regardless, the Minister should receive clear and accurate information about this fact prior to the authorization, given the risks to privacy interests of Canadians.

Recommendation no. 1: NSIRA recommends that CSE clearly explain, in its applications to the Minister, that:

- Network-based solutions acquire information relating to a Canadian or a person in Canada (IRTC), including information that interferes with the reasonable expectation of privacy (REP) of Canadians or persons in Canada; and,

- CSE subsequently uses, analyses, and retains this information for use in cybersecurity and information assurance activities.

Consent to CSE's cybersecurity solutions

50. As per paragraph 34(3)(b) of the CSE Act, one condition for the Minister to issue a

---

[43] Emphasis NSIRA's. See, for example, 2020-2021 authorization for CSE cybersecurity activities on federal infrastructures, paragraph 1(a).
[44] Emphasis NSIRA's. See, for example, 2020-2021 Application for CSE cybersecurity activities on federal infrastructures, paragraph 72.
[45] See, for example, *National Defence Act* at paragraph 273.65(1); Ministerial authorizations for CSE per the *National Defence Act* were required in order for CSE to intercept PCs. Archived copy of the NDA available online at: https://www.laws-lois.justice.gc.ca/eng/acts/N-5/20190712/P1TT3xt3.html.

cybersecurity authorization for federal infrastructures (27(1) of the CSE Act) is that there are reasonable grounds to believe that the consent of all persons whose information may be acquired could not be reasonably obtained. In the case of a cybersecurity authorization for non-federal infrastructures (27(2) of the CSE Act), CSE must obtain a written request of the given infrastructure owner or operator asking CSE to carry out the authorized activity.

51. As of May 2023, all authorizations since 2019 for cybersecurity activities on federal infrastructures included the following statement:

> "In accordance with standard government practice, federal institutions must advise authorized users of these information infrastructures that their device and/or network activity are being monitored for cybersecurity and information assurance purposes."[46]

This statement aligns with provisions set out in GC documents such as the Treasury Board Policy on Service and Digital. According to the Policy on Service and Digital, deputy heads of departments are responsible for informing authorized users of departmental electronic networks and devices of "Monitoring practices being applied by their own department and by SSC",[47] among other responsibilities.

Transparency toward, and cooperation with, system owners

Finding no. 4: NSIRA found that, due to a lack of clarity in its relationship with SSC, CSE did not obtain consent from system owners for its cybersecurity and information assurance activities in the way described to the Minister.

Finding no. 5: NSIRA found that SSC was not fully aware of its responsibilities as a system owner, as described in CSE's applications to the Minister.

Finding no. 6: NSIRA found that, despite the existence of a Memorandum of Understanding between CSE and SSC, there was a lack of clarity between the organizations on the implementation of agreed-upon commitments about NBS activities on networks operated by SSC.

52. The Chief's 2019-2020 and 2020-2021 applications to the Minister, for cybersecurity activities on federal infrastructures, state that "CSE deploys its HBS, NBS, and CBS capabilities only with the informed consent of the system owner of the federal institution's information infrastructure."[48] The subsequent two applications for cybersecurity activities on federal infrastructures—2021-2022 and 2022-2023—did not include the word 'informed' in this context.

53. While CSE obtains the consent of the NBS partner for NBS deployment, this does not usually include the specific departments or agencies linked to that network. For instance, SSC's Internet Interconnectivity Service (IIS) network had approximately 90 GC departments or agencies connected to it during the period of review, yet CSE's partnership was solely with SSC (system owner for the IIS network), rather than the various entities connected to SSC's IIS network. As such, SSC acts as a consent broker for the various departments or agencies connected to its network.

---

[46] Authorization for Cybersecurity Activities on Federal Infrastructures: 2019-2020 and 2020-2021 paragraph 2(d), 2021-2022 paragraph 37, 2022-2023 paragraph 34. Also in corresponding applications: for example, 2020-2021, paragraph 86, and 2021-2022, paragraph 15.

[47] TBS, Policy on Service and Digital, section 4.4.2.6, available online at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603. Further, as per section 4.4.3.1, the deputy head of SSC is responsible for managing tools to support the monitoring of departmental electronic networks and devices.

[48] Emphasis NSIRA's. Application for CSE cybersecurity activities on federal infrastructures: 2019-2020, paragraph 7; 2020-2021, paragraph 14.

54. Collaboration between CSE and SSC on NBS is longstanding. According to CSE, SSC is "actively involved with CSE on a variety of levels related to [the] NBS program", and SSC "is fully briefed on the NBS program", both upon initial deployment and through various formats and operational interactions. SSC, toward the end of the review, told NSIRA that "SSC has a solid understanding of the role that CSE plays in protecting and monitoring the Government of Canada network." SSC further stated that it trusts that "CSE provides SSC with the necessary information to enable SSC to respond to incidents and events effectively", while also emphasizing a strong relationship and "track record of timely and appropriate interventions." Nevertheless, in briefings and written responses over the course of the review, SSC indicated that it views NBS and the workings of CSE's cybersecurity sensors as "black boxes".[49] SSC also stated during the review that it is not provided with explanation about CSE cyber defence processes, procedure, risk, or technical information related to tools or services. Of note, SSC maintains its own suite of firewalls, in addition to the protection offered by CSE's CSIA program. While layering protections is a common cybersecurity practice, SSC's lack of visibility into CSE's defences could contribute to operational inefficiencies. For example, SSC described being unable at times to quickly attribute an apparent blocking action or unexpected network behaviour.

55. SSC further confirmed that it "does not have a specific process for advising departments of the NBS program", other than onboarding packages which "may contain boilerplate statements regarding the fact that systems are monitored for security purposes and that there is no presumption of privacy while working on a government system". SSC's practice in this case does not reflect what CSE described to the Minister in its applications for authorizations. Moreover, this does not align with SSC's responsibility per a March 2014 Memorandum of Understanding (MoU) between CSE and SSC, where it is agreed that SSC will inform its clients that "CSE may acquire their data, including personal information and/or private communications, while conducting cyber defence activities for SSC."[50]

56. CSE made assurances to the Minister through the Chief's application that CSE obtains system owners' consent to cybersecurity sensors, including NBS. In reality, SSC was broadly unaware of how CSE's cybersecurity activities operate, and SSC in turn did not—and was not able to—adequately inform clients that CSE may acquire their information in the course of CSE's authorized cybersecurity activities, including the collection and retention of personal information and the content of communications.[51] During the factual accuracy consultation for this report, CSE noted that this report "is the first time that CSE has been informed that SSC is not aware of its responsibilities as a system owner."[52]

57. The 2014 MoU between CSE and SSC sets out the terms and conditions under which CSE's cyber defence activities were conducted on systems and networks under SSC control. The MoU stipulates that SSC will "Ensure that SSC clients have been informed that CSE may acquire their data, including personal information and/or private communications, while conducting cyber defence activities for SSC." In turn, the MoU states that CSE will provide SSC with details about processes, procedure, technical information related to tools or services, and risks, prior to deployment on SSC networks or systems.

---

[49] SSC briefing responsive to NSIRA RFI-1, September 6, 2022; SSC written response to RFI-2, questions 3 and 4, March 6, 2023.

[50] CSE document, "Memorandum of Understanding between Communications Security Establishment (CSE) and Shared Services Canada (SSC)", page 2, March 27, 2014.

[51] During the review's factual accuracy consultation, SSC contested this characterization, in contrast to verbal and written statements from SSC throughout the review, as noted in paragraph 52.

[52] CSE also listed various mechanisms which, in CSE's view, have ensured that SSC remains aware of the NBS and CSE network defence capabilities. Such awareness was not reflected in NSIRA's interactions with members of various SSC teams during the review.

58. However, SSC initially stated during the review that the 2014 MoU was no longer in force, having been replaced by a 2018 MoU in support of the creation of the Cyber Centre and related transfer of resources. Yet the 2018 MoU pertains to organizational and financial considerations and does not make substantive mention of CSE's cyber defence sensors or how they operate. The lack of information about CSE's cyber defence activities in the 2014 MoU stands in contrast to MoUs received by NSIRA for [redacted] provided more substantive information about CSE cyber defence activities, including authorities and descriptions of the types of activities to be undertaken.[53]

59. In addition to SSC, other MoUs between CSE and its cyber defence partners date from before the CSE Act. For example, the most recent MoUs for NBS services, received by NSIRA during this review, between [redacted]. As per s. 81 of the CSE Act, CSE's MoUs established prior to the CSE Act continued in accordance with their terms after the coming-into-force of the CSE Act, and CSE confirmed its view that this was the case for the SSC MoU.

60. During the factual accuracy consultation at the final stages of the review, SSC informed NSIRA that—contrary to its initial statements—the 2014 MoU with CSE remained in effect. SSC further stated that it will "continue to work with CSE to ensure that the expectations outlined in the 2014 MoU remain aligned with updated Government of Canada policies."

Recommendation no. 2: NSIRA recommends that CSE renew its Memorandum of Understanding with SSC to ensure CSE and SSC meet their respective commitments, including any that CSE makes to the Minister regarding SSC's role in informing system owners about the NBS program.

Recommendation no. 3: NSIRA recommends that CSE update Memoranda of Understanding with all of its cybersecurity partners, to ensure these partners have consented to CSE cybersecurity activities, and to ensure these arrangements reflect, and conform to, contemporary governance authorities. CSE should continue these updates, as a standard practice, as authorities evolve.

Transparency toward system users

Finding no. 7: NSIRA found that CSE did not explain to the Minister why consent to CSE's cybersecurity activities could not reasonably be obtained from users of Government of Canada systems.

61. Broadly speaking, there are two groups who use GC systems: non-GC users (e.g.: the public, or those outside of the GC interacting with the GC), and GC users (e.g.: employees of GC institutions). For the first group, CSE adequately explains to the Minister, per paragraph 34(3)(b) of the CSE Act, why their consent cannot reasonably be obtained. However, there is no explanation to the Minister of either why consent cannot be obtained, or how consent is obtained, from *users* of GC systems (e.g., GC employees). This is despite the requirement in paragraph 34(3)(b) that the Minister must have reasonable grounds to believe consent of all persons whose information may be acquired could not reasonably be obtained.

[53] See, for example, [redacted] (CERRID #71886V3), and [redacted] (CERRID #162578).

62. There is no explicit legal requirement for CSE to inform users of GC systems that it acquires information from those systems pursuant to a cybersecurity authorization. CSE could explain to the Minister that it cannot reasonably obtain consent from these users. Instead of providing such an explanation, CSE's position to the Minister is that respective federal institutions are responsible for advising authorized users of GC information infrastructures that their devices or network activity are monitored for CSIA purposes.

63. In lieu of obtaining consent of all persons whose information may be acquired, it is important that appropriate notice be provided—particularly to the primary users of GC systems such as GC employees—that CSE may acquire and use information from those systems for cybersecurity purposes. CSE told NSIRA that consent *is* obtained from users of GC systems through a notification to these users that their device and/or network activity are being monitored for cybersecurity and information assurance purposes. CSE further stated that when a user acknowledges the notification by clicking an acceptance button, this demonstrates the user's consent. NSIRA did not verify the content of this notification, nor whether it is shown to all users of GC systems. SSC, for its part, took issue with the notion of consent in this context, pointing out that the Treasury Board policy requiring these notices "is focused on notification rather than consent."

Recommendation no. 4: NSIRA recommends that CSE explain to the Minister how consent to CSE's cybersecurity activities is obtained from users of Government of Canada systems, or otherwise explain why this consent could not reasonably be obtained.

Information from external sources for which there is a Reasonable Expectation of Privacy (REP) of a Canadian or person in Canada

64. Section 17 of the CSE Act allows CSE to acquire, use, and analyse information from the GII or from other sources in order to provide advice, guidance and services to help it protect both federal institutions' electronic information and information infrastructure, and electronic information and information infrastructures designated as being of importance to the Government of Canada (Systems of Importance, or SOIs). For example, CSE can acquire, use, and analyse publicly available information (PAI), defined in the Act as "information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise is available to the public on request, by subscription or by purchase."[54] Importantly, PAI does not include information in respect of which a Canadian or person in Canada has a reasonable expectation of privacy.

65. As per paragraph 23(1)(a) of the CSE Act, CSE is permitted to acquire and use PAI without seeking an authorization. If the acquired PAI contains IRTC, paragraph 24(a) of the CSE Act requires CSE to implement measures to protect privacy when using, analysing, retaining, or disclosing information acquired while conducting activities under its foreign intelligence or cybersecurity aspects of its mandate.[55] Some of these measures are described in Annex A.

66. A limit is applied to CSIA activities in subsection 22(4), which prohibits CSE from acquiring information from the GII in a way that contravenes any Act of Parliament or interferes with the

[54] CSE Act, section 2.
[55] Ministerial authorization for CSE cybersecurity activities on federal infrastructures 2019-2020, page 2.

reasonable expectation of privacy of a Canadian or person in Canada. For CSIA activities, CSE can only acquire information in this way if the acquisition is conducted under a Ministerial authorization issued in accordance with subsections 27(1) or (2) of the CSE Act. As such, CSE cybersecurity activities that risk interfering with a reasonable expectation of privacy of a Canadian or person in Canada can only be authorized on federal information infrastructures and systems designated as important to the Government of Canada.

Risk of acquiring information that contains a REP in sources of cybersecurity information outside of an authorization

Finding no. 8: NSIRA found that CSE's narrow application of subsection 22(4) of the CSE Act introduces legal and accountability risks and, in at least one instance, resulted in CSE acquiring information that may interfere with a reasonable expectation of privacy of a Canadian or person in Canada. This information was from a source acquired outside of the scheme of Ministerial authorizations.

Finding no. 9: NSIRA found that an incongruence between subsections 27(1) and 22(4) of the CSE Act prevents CSE from acquiring certain information from external sources such as commercial databases, where this information interferes with the reasonable expectation of privacy of a Canadian or person in Canada. Some of this information would enhance CSE's ability to fulfill its cybersecurity and information assurance mandate.

67. In addition to the tripartite sensors, CSE's cybersecurity information is complemented by information from SIGINT, disclosures,[56] agreements, and other publicly-available sources like commercial and open sources, including information and databases aggregated by data brokers. CSE provided NSIRA with a list of [redacted] external sources (other than CSE sensors or SIGINT sources) that yielded information used by CSE for activities related to federal cybersecurity authorizations during the review period.[57] [redacted] this type of information is a common practice for cybersecurity, as it allows the gathering of information from [redacted]

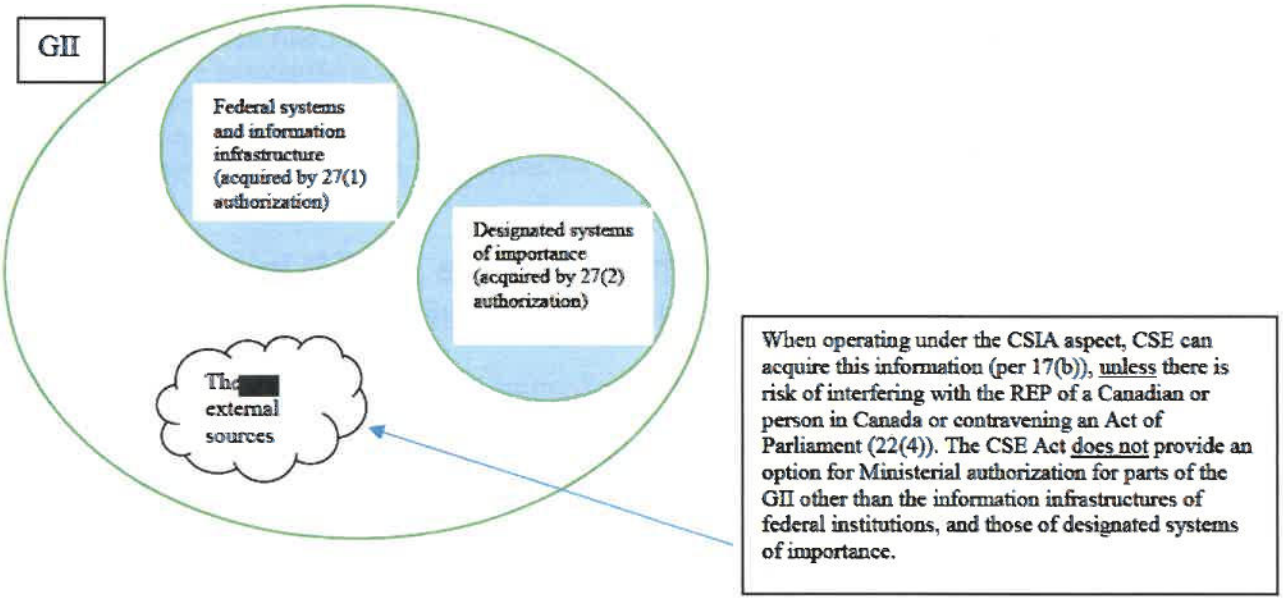
68. These [redacted] sources yield information from portions of the GII other than what CSE can access under subsection 27(1) and (2) authorizations.[58] This is visualized in Figure 3.

Figure 3: GII, and subsections 27(1) and (2) of the CSE Act:

[56] Disclosures can include those from client departments, as well as voluntary disclosures from other sources such as international CERTs, public disclosures of malware to mlwr.cyber.gc.ca, information shared by Five Eyes partners, and more.

[57] This information can be shared with other aspects of CSE's mandate. (From NSIRA Review 20-07, RFI-11: "[redacted] Generally, there are no contractual restrictions on use between aspects of the mandate, [redacted]")

[58] Specifically, subsection 27(1) allows for CSE to "access a federal institution's information infrastructure", and 27(2) allows CSE to "access an information infrastructure designated under subsection 21(1) as [a system of importance to the GC]".



69. Beginning in 2020-2021, the Chief's applications for federal cybersecurity authorizations mention that CSE combines cyber threat information from federal institutions with sources as described above, including publicly available information.[59] Shortly thereafter, in early 2021, CSE initiated internal discussion between its operational, compliance, and legal groups about questions raised regarding open source information that had a potential to infringe on a REP of a Canadian or person in Canada, in the context of acquisition for foreign intelligence (s. 16) activities.

70. CSE takes the position that the CSE Act "does not distinguish between a lower, or higher, reasonable expectation of privacy." In other words, regardless of the degree to which, or likelihood that, a REP might be interfered with, and regardless of the mandate aspect under which the REP might be interfered with, CSE nevertheless requires an authorization as per subsections 22(3) and 22(4) of the CSE Act if there is even a low risk of REP in information being acquired.

71. In CSE's application per subsection 27(1) for the 2022-2023 Cybersecurity Authorization for Activities on Federal Infrastructures, CSE noted—for the first time—that CSE sought to acquire cybersecurity information from third party providers (external sources) which "may have a low risk of interfering with the reasonable expectation of privacy of a Canadian or person in Canada."[60] The application states that this issue was recently recognized by CSE.

72. CSE's application to the Minister stated that "When CSE encounters this information [redacted], it is arguable that this activity does not need to take place under an Authorization as CSE is not directly acquiring information from the GII."[61] CSE developed this view based on the [redacted] rationale that there are "strong arguments" that searches [redacted] "would not constitute an acquisition by CSE of information with an REP from the [GII]".[62] [redacted] still recommended that CSE "list these activities as an acquisition technique in an authorization," even

[59] NSIRA notes that the 2019-2020 application does not mention this fact. Applications for CSE cybersecurity activities on federal infrastructures: 2020-2021, paragraph 13; 2021-2022, paragraph 19. The 2022-2023 application makes significant reference to this fact, including in paragraph 6, as well as in paragraphs 63-74, which were not approved by the Intelligence Commissioner.
[60] Application for CSE cybersecurity activities on federal infrastructures 2022-2023, Section VII, paragraph 69.
[61] Ibid.
[62] [redacted]

while recognizing that the cybersecurity authorization regime as per the *CSE Act* cannot be applied to this CSE activity.[63] Ultimately, as mentioned, CSE listed the activities as an acquisition technique in its application to the Minister.

73. After the Minister issued the authorization based on this application, and it was sent to the Intelligence Commissioner (IC) for approval, the IC did not approve the portion of the authorization pertaining to the acquisition of information from external sources which may interfere with the REP of a Canadian or person in Canada. The IC concluded that there was no rationale or information provided by CSE to the Minister to explain how the acquisition of information from third parties, that risked interfering with a REP, could be authorized by subsection 27(1). The IC commented that "The language of subsection 27(1) does not, *prima facie* (at first view), contemplate or permit the issuance of an authorization outside the scope of accessing a federal institution's information infrastructure."[64] NSIRA further notes that the acquisition in question could not, also, be covered under a subsection 27(2) authorization. The CSE Act, as drafted, limits CSE's CSIA activities on most of the GII—other than federal information infrastructures and SOIs—to activities that do not require an authorization.

74. Table 1, below, provides a timeline of events pertaining to this issue:

Date	Event
September 2, 2020	Cyber Centre [redacted]
March 29, 2021	A CSE group [redacted]
May 26, 2022	Chief CSE signs 2022-2023 application for cybersecurity activities on federal infrastructures, which contains new language about acquiring information from the GII that may risk interfering with the REP of a Canadian or person in Canada.
June 1, 2022	Minister of National Defence issues the 2022-2023 authorization, per ss. 27(1) of the CSE Act, for cybersecurity activities on federal infrastructures, which contains new language about acquiring information from the GII that may risk interfering with a REP.
June 9, 2022	[redacted]
June 27, 2022	Intelligence Commissioner approves the 2022-2023 application for cybersecurity activities on federal infrastructures, except for the section of the application about acquiring information from the GII that may risk interfering with a REP.

75. Despite the IC decision to not approve the section of the Ministerial authorization pertaining to acquisition of cybersecurity information from external sources which may interfere with the REP of a Canadian or person in Canada, CSE nevertheless continued to acquire information from third party sources.[65] CSE continued the acquisition of information from these sources based on CSE's view that the information was not an acquisition by CSE of information from the GII—and thus CSE's ingestion was not, under this view, prohibited by subsection 22(4) of the CSE Act.[66, 67] The decision to continue

[63] Ibid., page 6.
[64] Intelligence Commissioner, File 2200-B-2022-01, page 10. See figure 3.
[65] CSE confirmed to NSIRA that these sources continued to be acquired under the CSIA (s. 17) aspect of CSE's mandate.
[66] According to this CSE view, CSE could continue to acquire these sources under paragraph 17(b) of the CSE Act without need for Ministerial authorization.
[67] Interestingly, the 2022-2023 Ministerial authorization circulated within CSE was not modified nor reissued to remove the language that was not approved by the Intelligence Commissioner. The language which was not approved remained in the 2022-2023 Ministerial authorization throughout the authorization period, for example in paragraphs 47 and 48 of the authorization. In comparison, the corresponding application was modified, with a caveat noting that the activities requested in the novel section were not approved by the Intelligence Commissioner.

to acquire this external information outside of an authorization after the IC did not approve those same activities is concerning—especially in light of the nature of at least one of these sources, as discussed below.

76. NSIRA's investigation into this issue began at a time when CSE was also examining the matter; information thus evolved as CSE determined its approach. In November 2022, CSE stated that it was assessing the privacy considerations of information used for CSIA activities from sources other than CSE sensors, including assessments of the degree to which there may be a REP in this information. According to CSE:

> "Where a source was [redacted] [CSE is] developing a framework to understand the potential implications for REP, noting that the information in these cases [redacted]. In cases where CSE directly acquired the information and the information may contain IRtC, techniques are being developed to prevent the collection of IRtC and subsequently any interference with REP."

CSE also acknowledged that "REP is expected to evolve over time both through case law and use cases", and that CSE "will continue to monitor, learn and adjust accordingly." Furthermore:

> "The Authorities, Compliance and Transparency branch (ACT) has been working internally [redacted] to catalogue incoming data sources used by the Cyber Centre to determine types of data, where the data comes from (i.e.: GII or not), and how Cyber Centre acquires it ([redacted] disclosure or other means) … Based on this information, ACT, [redacted] worked to evaluate these sources as to whether the data source might contain IRtC. In general, the information in these [redacted] is technical in nature and would present a low-risk to REP."[68]

77. CSE later stated, in May 2023, that identifying a framework for assessing or defining REP was difficult, in part due to a lack of jurisprudence on REP in a cyber context. Instead, in practice, operators had been issued guidance such that if they identify changes in their [redacted] information sources, the operators are to consult with CSE's internal compliance unit. CSE further explained that, while information collected from the GII which could potentially interfere with the REP of a Canadian or person in Canada was within CSE's holdings prior to being recognized and disposed of, the same privacy mitigation measures that it applies to all IRTC would also be applied—on a case-by-case basis—to any information that interferes with a REP if discovered by analysts. CSE noted that, in cases where information that interferes with a REP is identified in CSE's holdings, it is deleted. As of mid-2023, CSE Operational Policy was working to develop a framework to help provide additional guidance for operators related to open source acquisition. CSE also told NSIRA that it conducts due diligence to ensure that [redacted] are "reputable" and operating lawfully, though CSE was unable to clearly articulate nor provide specific examples of how this had been, or would be, done.

78. CSE's internal compliance unit, which was directly engaged on this issue, conducted (inter alia) a 'categorization exercise' that examined the [redacted] external sources of cybersecurity information for whether those sources constituted an acquisition *by* CSE of information *from* the GII.[69] CSE's categorization exercise proceeded "based on the understanding that information lawfully acquired [redacted], then obtained by CSE [redacted] in support of CSE's mandate, would not be considered an acquisition from the GII by CSE as set out in the CSE Act, and could therefore be acquired without consideration of a Ministerial Authorization."[70] CSE concluded that all but [redacted] of the [redacted] external sources were not acquired by CSE from the GII.

---

[68] Emphasis NSIRA's.

[69] Of note, this categorization exercise occurred after the IC decision.

[70] When asked by NSIRA about how CSE ensured that the third-party vendors/publishers were acquiring information lawfully, CSE was unable to provide any specific examples aside from hypothetical scenarios. NSIRA received no evidence to suggest that CSE meaningfully assessed the lawfulness of data brokers and other vendors from which it acquired cybersecurity information necessary for its CSIA activities.

Importantly, as a result, CSE did not formally examine whether the [redacted] sources contained information that risked interfering with the REP of a Canadian or person in Canada, despite confirming that at least one of these sources included information that risked doing so. Put plainly, CSE's approach was to address questions pertaining to REP in this context after information that might interfere with a REP was identified as being in CSE's holdings, rather than proactively.

79. NSIRA examined some of the [redacted] external sources of cybersecurity information (sources not covered by a Ministerial authorization). In particular, NSIRA focused on [redacted] CSE acquires information from [redacted] in various forms, including threat reports, IOC [redacted], and searchable datasets. Given the nature of this information, it is likely that some of this information interfere with a REP of a Canadian or person in Canada—including information other than GC information.

80. After CSE's categorization exercise, CSE ultimately decided that in this specific case its "querying into [redacted] datasets and extracting information is akin to an acquisition by CSE from the GII", but that measures can and are being taken to prevent the acquisition of information from those datasets that might interfere with the REP of a Canadian or person in Canada. In CSE's view, so long as these measures are in place, and the information being acquired does not interfere with the REP of a Canadian or person in Canada, CSE can continue that acquisition without a Ministerial authorization. Given CSE's approach to address REP information once it is identified in CSE's holdings, it is possible that that CSE could acquire information that interferes with the REP of a Canadian or person in Canada, outside of an authorization, despite the prohibition in subsection 22(4) of the CSE Act.

81. More broadly, CSE's general conclusion that acquisition of information from external sources—for example, [redacted]—does not constitute an acquisition by CSE of information from the GII raises questions. Per section 2 of the CSE Act, the GII is defined broadly to include "electromagnetic 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." Intuitively, actively seeking information—for example [redacted]—could appear akin to an acquisition. CSE's position, that its ingestion of information from such external sources does not constitute an acquisition from the GII, is thus tenuous and may introduce risk.

82. The acquisition of cybersecurity information sources outside of Ministerial authorizations that *do not* risk interfering with the REP of a Canadian or person in Canada nor contravene an Act of Parliament, does not pose compliance concerns. However, CSE's current practice of not assessing information sources for potential interference with a REP prior to their acquisition introduces the risk that CSE could retain unassessed data containing information subject to a REP—ingested outside of a legislative scheme—indefinitely. Parliament contemplated that it would be necessary for CSE to acquire, use and retain this type of REP-containing information in the course of CSE's CSIA activities; the CSE Act ss. 22(4) prohibits this acquisition, use, and retention unless these are first authorized by the Minister and approved by the IC. This Ministerial accountability regime is thus central to the underlying lawfulness of these CSIA activities. Yet CSE's narrow interpretation of ss. 22(4) excludes some of these intrusive and extraordinary activities from this regime. Furthermore, CSE did not specify whether its interpretation of the larger provisions rests on a particular interpretation of the term "acquisition", or "Global information infrastructure". This raises questions as to whether the interpretation of this prohibition, and the individual terms within it, will impact activities in other aspects of CSE's mandate.

83. In addition to the 2022 Intelligence Commissioner decision on the Ministerial authorization for CSIA activities on federal systems, a subsequent 2023 IC decision on the corresponding authorization

for the 2023-2024 period examined the 2022 decision, and evaluated the Ministerial authorization scheme applicable to CSIA activities more generally.[71] The two IC decisions, in addition to the facts as described in this report, demonstrate—in effect—that the CSIA activities which may be authorized in accordance with ss. 27(1) are more limited than the activities prohibited by ss. 22(4). The 27(1) authorization is limited by the links to "federal institution's information infrastructure." In contrast, the respective analogous statutory prohibition and Ministerial authorization(s) applicable to the foreign intelligence aspect of CSE's mandate appear symmetrical. In other words, in the case of foreign intelligence, activities prohibited under ss. 22(3) may be authorized by the Minister under s. 26.

84. The incongruence between ss. 22(4) and 27(1) appears to limit activities, such as the acquisition of certain information from external sources, which would support the CSIA aspect of CSE's mandate and would not otherwise be precluded by the Act. In an April 2023 document provided to the Minister and the Intelligence Commissioner, the Chief of CSE characterized this incongruity as a "legislative drafting oversight."[72]

Recommendation no. 5: NSIRA recommends that CSE reconsider whether limits on the acquisition by CSE of information from the global internet infrastructure (as per subsection 22(4) of the CSE Act) apply to information from third-party data sources. This should include an assessment of whether section 8 of the *Charter of Rights and Freedoms* may be engaged, as well as cases where third-party data sources may contain information that interferes with the reasonable expectation of privacy of a Canadian or person in Canada.

Recommendation no. 6: NSIRA recommends that, in order to continue these acquisition activities that are necessary for cybersecurity and information assurance (CSIA) purposes, CSE assess its current sources of CSIA information—that are acquired outside of an Authorization—for interference with the reasonable expectation of privacy of a Canadian or person in Canada. This assessment should be repeated as required to ensure such information is not acquired without a valid Ministerial authorization.

Recommendation no. 7: NSIRA recommends that section 27 of the CSE Act be amended to permit the Minister to authorize CSE to acquire information that is necessary for CSE's cybersecurity and information assurance aspect (but which may contain information that interferes with the reasonable expectation of privacy of a Canadian or person in Canada, or contravene an Act of Parliament), from sources other than federal information infrastructures and systems of importance to the Government of Canada.

---

[71] Intelligence Commissioner file no. 2200-B-2023-02.
[72] As cited in Intelligence Commissioner file no. 2200-B-2023-02, paragraph 79.

V. CONCLUSION

85. CSE, and the Canadian Centre for Cyber Security within it, operate a comprehensive and integrated ecosystem of cybersecurity systems, tools, and capabilities. This ecosystem protects the electronic information and information infrastructures of Canadian federal institutions and applicable infrastructures deemed important to the Government of Canada, with a design that incorporates measures meant to protect the privacy of Canadians and persons in Canada.

86. In the context of NSIRA's review mandate it is particularly salient that NBS sensors, and related activities under the CSIA program, are certain to acquire information related to Canadians or persons in Canada, including information that interferes with the reasonable expectation of privacy of a Canadian or a person in Canada. NSIRA made findings and recommendations in two main thematic areas: transparency to the Minister about the nature of elements of some NBS-related activities, and a specific issue with regard to an information acquisition activity from external sources, which CSE continued to conduct even after this activity was not approved by the Intelligence Commissioner.

87. In the latter case, the issue resulted from an incongruence in CSE's legislation that appears to limit the ability for an authorization to be issued under the CSIA aspect of CSE's mandate for the acquisition activity, despite the important value of information from this acquisition to CSE's ability to protect electronic information and information infrastructures.

88. NSIRA continued to face challenges from CSE regarding timeliness and access to information during the first half of the review, though was satisfied with CSE timeliness and access in the second half of the review. Despite continuing discussions with CSE on required improvements to NSIRA's access to CSE information, NSIRA was able to verify information received during the review in a manner that met NSIRA's expectations.

89. The information examined by NSIRA during this review also supported NSIRA's internal knowledge-building about CSE; this foundation will enable more specific review focuses in the future.

ANNEX A: Lifecycle of Information

90. This Annex describes how information travels through CSE's cyber defence ecosystem, beginning with initial collection—in this case through network-based sensors—through to the publication or sharing of reporting based on that information. Some information in this section may be current only as of the end of NSIRA's review period (June 17, 2021).

91. CSE's CSIA ecosystem collects extensive data, including network packets, host activity events, and logs. This data moves through four main steps: (1) collection; (2) analysis; (3) retention and disposal; and (4) reporting and use. The data moves through different networks in these steps, from unclassified partner networks to CSE networks. Each step involves multiple technical systems, operating either automatically or under the direction of human analysts. The processing and analysis of cybersecurity data is not specific to a given sensor program or source of information; steps 2–4 apply to all sources of cybersecurity data. Throughout these various steps, CSE has implemented various measures to protect the privacy of Canadians and persons in Canada, including assessments for relevance, necessity, and/or essentiality, access control to sensitive information, retention limits, and automation.[73] Although NSIRA did not examine all of these measures nor fully verify the details of their implementation, some of these measures are described in this section.

Collection

92. The data on which CSE's CSIA systems operate is collected directly, through the [redacted] of [redacted] NBS, [redacted] cloud-based solutions (CBS) and host-based solutions (HBS). A copy of the data is sent to processing systems on both CSE's classified and unclassified networks. When received by CSE's systems, all collected data is considered unassessed, described by CSE and in this section as "raw".

93. The raw data is copied and sent through several different systems for processing. [redacted][74]

94. At this stage, the processed data is still considered unassessed, as it has only been processed by automated processes, not yet viewed by an analyst.

Analysis

95. CSE cybersecurity analysts use various tools to access cyber defence data. These tools can search extracted metadata based on different criteria, and can be run manually or automatically, on a defined schedule, via scripts written by analysts. From these tools, analysts can access the raw data

[73] CSE provided examples of 12 different privacy protection measures applied when conducting authorized CSIA activities. NSIRA did not evaluate the effectiveness of these measures.

[74] [redacted]

[redacted]

96. In addition to the tripartite sensors, CSE's cybersecurity information is complemented by information from SIGINT, disclosures,[75] agreements, and other publicly-available sources like [redacted] open sources.[76] Analysts can query these [redacted] sources, manually or automatically, in combination with raw data collected by CSE sensors, to produce mitigation actions and reporting.

97. When an analyst identifies data that meets CSE policy thresholds for use, analysis, or retention, they retain it in CSE's cyber defence knowledgebase.[77] To be retained, NBS data must meet CSE's threshold of essentiality (discussed further in the section on retention and disposal), due to CSE's assumption that all NBS data includes IRTC. Analysts must tag data to explain why it is being retained, choosing from one of three possible options. Data can be retained because it: [redacted]

98. Given the amount and sensitivity of the information available through the various analysis tools, access is limited to CSE staff that have completed the annual Acknowledgement of Legal and Policy Requirements (ALPR) training and test.[78] Various actions in the system are logged (for example, all queries to access processed data are logged and retained for [redacted]) to enable auditing.[79]

99. In some cases, automated processes assess data on behalf of analysts, for example in Assemblyline, a malware analysis tool built by CSE.[80] Assemblyline performs static and dynamic analysis of files, including email attachments, to identify malware or other malicious content. It analyses all extracted files automatically, and alerts analysts of files suspected to be malicious. Analysts can then use an interface to review the potentially malicious files, extracting and retaining data if appropriate. Analysts can also automate the identification of malicious files by creating filters in Assemblyline. Filters identify files with certain characteristics, then deem any future files with the same characteristics as malicious, automatically retaining the data.

Retention and disposal

100. Raw data must, according to CSE policy, be deleted [redacted] of acquisition".[81] Though precise timing differs by system, most raw data is deleted much sooner than [redacted] after

---

[75] Disclosures can include those from client departments, as well as voluntary disclosures from other sources such as international CERTs, public disclosures of malware to mlwr.cyber.gc.ca, information shared by Five Eyes partners, and more.

[76] CSE uses [redacted] sources to complement its analysis. This information can be shared with other aspects of CSE's mandate. Further, "[redacted]

[77] This knowledgebase contains assessed and retained CSIA information, as well as assessed foreign intelligence information relevant to cybersecurity purposes. Information stored in this knowledgebase can also be sent to clients and partners in various forms, and can be used to inform mitigation actions against cyber threats.

[78] The majority of staff on the ALPR list in 2020 and 2021 worked for CSE's CSIA aspect ([redacted]% and [redacted]% respectively); the remainder worked in the foreign intelligence aspect ([redacted]% and [redacted]%) or other units of CSE ([redacted]% and [redacted]%). Staff on the ALPR list working in the CSIA aspect represented [redacted]% and [redacted]%, respectively, of the CSIA aspect's total headcount; in foreign intelligence, they represented [redacted]% and [redacted]%.

[79] NSIRA notes that, though CSE has clearly implemented extensive logging in its systems, it is unclear how CSE makes use of it on an ongoing basis – when requesting certain calculations or responses based on audit logs, CSE indicated it would require significant effort to make the logs usable. As viewed by NSIRA during a CSE technical demonstration, CSE's ability to audit the information captured in logs may not be robust, and it may not necessarily be occurring regularly across the NBS program.

[80] A version of Assemblyline is available online at: https://www.cyber.gc.ca/en/tools-services/assemblyline.

[81] MPS Cybersecurity, November 2020, section 12.2.

acquisition.[82]

101. Files processed by Assemblyline have a [redacted] approach to retention: [redacted]

102. CSE has different standards for data retention, depending on its sensitivity, escalating from relevance through necessity to essentiality:[83]

- Relevance: "Information that can be used to help protect federal systems or [systems of importance] and the electronic information they contain."
- Necessity: Information which is "required for the understanding of malicious cyber activities", but without which CSE *can* still identify, isolate, prevent, or mitigate harm.
- Essentiality: Information without which CSE cannot identify, isolate, prevent, or mitigate harm.

103. In the case of data acquired by NBS, CSE treats all of the information as IRTC. In this case, the policy standard for retention is essentiality, and analysts retaining data must justify its retention at that standard. This is met, as previously noted, by selecting one of three reasons: malicious activity, situational awareness, or capability development.[84] These are retained according to corporate retention requirements, either deleted or transferred to Library and Archives Canada after 10–30 years, depending on their nature.

104. The treatment of all NBS information as IRTC also has implications for disclosure. According to CSE, because any IRTC that has been retained by CSE has already been deemed as "essential", this IRTC can be disclosed so long as it is "necessary" to do so.[85] CSE considers this to be a "double" threshold of essentiality and necessity when IRTC is obtained under authorization.

105. At this stage, data in the knowledgebase is considered assessed, as it has been processed either directly by an analyst or indirectly, according to rules created by an analyst. It can then be used for cyber defence outputs, whether reporting or defensive actions.

Reporting and use

106. When an analyst, or automated tradecraft operating from analyst instruction, identifies a threat based on cyber defence data (e.g., [redacted]), they can generate a tasking for the Dynamic Defence system. This tasking will then be applied [redacted]. GC departments receiving cyber defence services from CSE can access limited information about mitigation rules applied to their infrastructure.

107. Reporting can take a variety of forms, from unclassified indicators of compromise (IOCs), including malicious IP addresses or domain names, to more substantial releasable cybersecurity products, such as incident reports [redacted].

---

[82] CSE POC report, "Review of Data Retention in Cyber Centre Systems". While the systems were generally found to comply with data retention rules, usually deleting data within [redacted], the report describes several compliance incidents indicating that, on occasion, raw data is found in systems [redacted] since its collection. This is generally due to software upgrades or misconfigured deletion scripts. In these cases, a compliance incident process ensues, with the data deleted at the end.

[83] MPS Cybersecurity, November 2020, Annex E - Definitions.

[84] These correspond to justifications provided in MPS Cybersecurity, November 2020, section 9.2.

[85] CSE document: "Background on necessary, essential", May, 2018.

- Report development begins on the classified network. A report can simply consist of [redacted] Managers verify the analysis, confirming, for example, that all supporting evidence for a report was retained.[86] With sanitization[87] and approval, reports can be transferred to unclassified networks for dissemination beyond CSE.
- Approved reports, depending on their nature and content, can be disseminated manually to a variety of partners, including: Five Eyes [redacted]; GC departments; Canadian critical infrastructure organizations.
- IOCs can be disseminated automatically to the same partners. IOCs are exchanged in near real-time through Aventail, [redacted]

108. Under the CSIA aspect of its mandate, CSE shares information extensively, both internally and externally to the GC—provided that the information is relevant to CSE's CSIA aspects, and it is essential to share this information with another entity. In the case of IRTC, this sharing is enabled by Ministerial Order,[88] which authorizes CSE to share IRTC acquired through its CSIA aspect to persons or classes of recipients designated by the Minister.[89] IRTC is generally disclosed only to the system owner of an affected system for victim notification (e.g., to identify an infected computer).

109. CSE told NSIRA that it removes "any personal information", i.e.: Canadian Identifying Information, IRTC, and private communications, from reporting before it is shared with any partner, though CSE later told NSIRA that this may not always be the case when [redacted]. NSIRA viewed some examples of CSE's removal (suppression) of personal information in viewing different kinds of cybersecurity reports, including during a technical demonstration. CSE may disseminate reports containing non-IRTC information to a broader audience, as is the case when sharing IoCs through AVENTAIL to private and public sector entities.[90]

110. In accordance with a Ministerial Order under s. 45 of the CSE Act,[91] other entities inside and outside of Canada, including but not limited to Five Eyes entities, can receive unsuppressed IRTC information from CSE.[92] In these cases, IRTC is shared in the form of releasable cybersecurity products.[93] Per CSE internal policy,[94] as well as the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, CSE must conduct a mistreatment risk assessment when it shares information with foreign nations that could identify an individual, either directly or indirectly. NSIRA did not closely examine this or other topics related to the disclosure of cybersecurity information outside of CSE.

---

[86] The extent of retained evidence can vary widely. During a CSE demonstration, for example, NSIRA observed that [redacted] was retained, [redacted] Information [redacted] were subsequently used to substantiate a [redacted] report. While [redacted] were of clear relevance to the report, it is unclear why [redacted] was retained, [redacted]

[87] "Sanitization is the process of editing [...] material to permit dissemination to non-indoctrinated persons." MPS Foreign Intelligence, February 2021, section 25.8.

[88] *CSE Act*, section 44.

[89] CSE Act, section 45.

[90] In assessing information dissemination for the purposes of this review, NSIRA obtained screenshots of the relevant cyber knowledge bases, and received CSE releasable cyber security products as well as their approval authorities.

[91] CSE Ministerial Order, "Designating Recipients of Information Relating to a Canadian or Person in Canada Acquired, Used, or Analyzed Under the Cybersecurity and Information Assurance Aspects of the CSE Mandate", 13 August, 2021.

[92] As per the said s.45 Ministerial Order, CSE can share IRTC with designated persons or classes of persons as described in the Order, if the disclosure is necessary to help protect the electronic information and information infrastructures of federal institutions and SOIs (as designated pursuant to s. 21(1) of the *CSE Act*).

[93] MPS cybersecurity 2022 section 24.4.3

[94] Ibid., section 10.4.

ANNEX B: Cross-aspect use of cybersecurity information

111. NSIRA's 2020 Review of information sharing across aspects of CSE's mandate (review no. 20-07) examined CSE's legal authority for internal information sharing within CSE between the foreign intelligence and the CSIA aspects of its mandate, with a particular focus on IRTC.[95] NSIRA found that CSE's policy framework for such sharing was compliant with the CSE Act; per CSE policy, an assessment of IRTC's relevance, essentiality, or necessity to each aspect is required for sharing information across the aspects.

112. As described in the Chief's applications to the Minister, information acquired under the authorization for cybersecurity activities on federal infrastructure "may also be used by CSE for other purposes authorized under the CSE Act. For instance, the information may be used to enable any other authorized activities under foreign intelligence or active and defensive cyber operations authorizations."[96] CSE internal policy for cybersecurity further elaborates that:

> Subject to conditions imposed by clients or disclosing entities, information assessed as relevant, necessary or essential and retained under the cybersecurity aspect of CSE's mandate may be used by CSE personnel operating under another aspect of CSE's mandate, with the exception of the Assistance mandate. The use of this information by another aspect must still align with the cybersecurity aspect (i.e., it is being used for the purpose of helping to protect electronic information or infrastructures of federal institutions or SOIs). This is considered a consistent use of the information by CSE.[97]

According to section 16 of the CSE Act, the foreign intelligence aspect of CSE's mandate is to "acquire, covertly or otherwise, information from or through the [GII], including by 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." These intelligence priorities include some subjects which are directly relevant to the CSIA aspect of CSE's mandate, for example "[redacted]", as well as "[redacted]" and "[redacted]".[98]

113. One example of CSE foreign intelligence use of *assessed* CSIA information is [redacted] CSE could also use assessed CSIA information for defensive or active cyber operations, so long as those operations are linked to a cybersecurity purpose—such as a cyber operation targeting a cybercriminal actor that may pose a threat to Canadian systems. According to CSE, SIGINT analysts can also access *unassessed* CSIA information, including information collected under cybersecurity authorizations (per ss. 27(1) or (2)). For example, [redacted]. However, CSE told NSIRA that when SIGINT personnel access or conduct queries of raw CSIA information, they are doing so under the CSIA aspect of CSE's mandate.

114. Similarly to CSE's cybersecurity authorizations, all of CSE's authorizations for foreign intelligence (FI) activities (ss. 26(1) of the CSE Act) mention cybersecurity, as well as links between foreign intelligence information and CSIA activities. All such authorizations state that information

---

[95] NSIRA review 20-07.
[96] Application for cybersecurity activities on federal infrastructure, 2020-2021, paragraph 58. Paragraph 59 implies these activities would be auditable.
[97] CSE MPS Cybersecurity, February 2022, section 26.2.
[98] Minister of National Defence, Ministerial Directive to CSE on the Government of Canada Intelligence Priorities for 2021-2023, issued August 13, 2021.

acquired under them that is identified as being IRTC "will be used, analysed, or retained only if the information is essential to international affairs, defence or security, including cybersecurity."[99] CSE's internal policy clarifies that:

> The central consideration when disseminating foreign intelligence information for use under the cybersecurity aspect of CSE's mandate is the concept of consistent use—information acquired by CSE under the foreign intelligence aspect of CSE's mandate must be used for FI purposes, and may then be shared to recipients acting under cybersecurity authorities if they are eligible to receive and use that information to fulfill their mandated activities.
>
> In order to release FI under the cybersecurity aspect of CSE's mandate … The information must be assessed to be of FI value in support of GC intelligence priorities; IRtC may only be shared with cybersecurity personnel if they meet the essentiality test for FI, as well being assessed as necessary for cybersecurity activities …[100]

For example, CSE SIGINT analysts can [redacted], meaning that CSIA analysts can act on this information to protect systems cyber threats. Thus, cybersecurity information acquired under the foreign intelligence aspect can be shared with and used by CSE for the purposes of the CSIA aspect.

[99] For example, this language appears in all foreign intelligence authorizations issued to CSE in 2021-2022. Emphasis NSIRA's.
[100] CSE MPS Foreign Intelligence, section 26.9, February 18, 2021 (version 5.0).

ANNEX C: Findings & Recommendations

Findings

Finding no. 1: NSIRA found that CSE operates a comprehensive and integrated ecosystem of cybersecurity systems, tools, and capabilities to protect against cyber threats, with a design that incorporates measures meant to protect the privacy of Canadians and persons in Canada.

Finding no. 2: NSIRA found that CSE treated all network-based solutions (NBS) information as information related to a Canadian or a person in Canada (IRTC), and applied measures intended to protect privacy to all NBS-acquired information.

Finding no. 3: NSIRA found that information acquired through NBS will, by its nature, always include information related to a Canadian or person in Canada (IRTC) and is certain to include some information for which there is a reasonable expectation of privacy (REP) of a Canadian or person in Canada. This was not transparently communicated in corresponding applications to the Minister.

Finding no. 4: NSIRA found that, due to a lack of clarity in its relationship with SSC, CSE did not obtain consent from system owners for its cybersecurity and information assurance activities in the way described to the Minister.

Finding no. 5: NSIRA found that SSC was not fully aware of its responsibilities as a system owner, as described in CSE's applications to the Minister.

Finding no. 6: NSIRA found that, despite the existence of a Memorandum of Understanding between CSE and SSC, there was a lack of clarity between the organizations on the implementation of agreed-upon commitments about NBS activities on networks operated by SSC.

Finding no. 7: NSIRA found that CSE did not explain to the Minister why consent to CSE's cybersecurity activities could not reasonably be obtained from users of Government of Canada systems.

Finding no. 8: NSIRA found that CSE's narrow application of subsection 22(4) of the CSE Act introduces legal and accountability risks and, in at least one instance, resulted in CSE acquiring information that may interfere with a reasonable expectation of privacy of a Canadian or person in Canada. This information was from a source acquired outside of the scheme of Ministerial authorizations.

Finding no. 9: NSIRA found that an incongruence between subsections 27(1) and 22(4) of the CSE Act prevents CSE from acquiring certain information from external sources such as commercial databases, where this information interferes with the reasonable expectation of privacy of a Canadian or person in Canada. Some of this information would enhance CSE's ability to fulfill its cybersecurity and information assurance mandate.

Recommendations

Recommendation no. 1: NSIRA recommends that CSE clearly explain, in its applications to the Minister, that:

- Network-based solutions acquire information relating to a Canadian or a person in Canada (IRTC), including information that interferes with the reasonable expectation of privacy (REP) of Canadians or persons in Canada; and,
- CSE subsequently uses, analyses, and retains this information for use in cybersecurity and information assurance activities.

Recommendation no. 2: NSIRA recommends that CSE renew its Memorandum of Understanding with SSC to ensure CSE and SSC meet their respective commitments, including any that CSE makes to the Minister regarding SSC's role in informing system owners about the NBS program.

Recommendation no. 3: NSIRA recommends that CSE update Memoranda of Understanding with all of its cybersecurity partners, to ensure these partners have consented to CSE cybersecurity activities, and to ensure these arrangements reflect, and conform to, contemporary governance authorities. CSE should continue these updates, as a standard practice, as authorities evolve.

Recommendation no. 4: NSIRA recommends that CSE explain to the Minister how consent to CSE's cybersecurity activities is obtained from users of Government of Canada systems, or otherwise explain why this consent could not reasonably be obtained.

Recommendation no. 5: NSIRA recommends that CSE reconsider whether limits on the acquisition by CSE of information from the global internet infrastructure (as per subsection 22(4) of the CSE Act) apply to information from third-party data sources. This should include an assessment of whether section 8 of the *Charter of Rights and Freedoms* may be engaged, as well as cases where third-party data sources may contain information that interferes with the reasonable expectation of privacy of a Canadian or person in Canada.

Recommendation no. 6: NSIRA recommends that, in order to continue these acquisition activities that are necessary for cybersecurity and information assurance (CSIA) purposes, CSE assess its current sources of CSIA information—that are acquired outside of an Authorization—for interference with the reasonable expectation of privacy of a Canadian or person in Canada. This assessment should be repeated as required to ensure such information is not acquired without a valid Ministerial authorization.

Recommendation no. 7: NSIRA recommends that section 27 of the CSE Act be amended to permit the Minister to authorize CSE to acquire information that is necessary for CSE's cybersecurity and information assurance aspect (but which may contain information that interferes with the reasonable expectation of privacy of a Canadian or person in Canada, or contravene an Act of Parliament), from sources other than federal information infrastructures and systems of importance to the Government of Canada.