

TOP SECRET // CEO



**National Security
and Intelligence
Review Agency**

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

NSIRA's Review of the Lifecycle of CSIS's Warranted Information

NSIRA // Review 22-07

15(1)(f) **Table of Contents**

List of Acronyms	ii
Glossary of Terms	iii
Executive Summary	iv
1. Introduction	1
Authority	1
Scope of the Review	1
Methodology	1
Review Statements	2
2. Background	2
3. [*] History, Development, and First Warranted Use	3
What is [*] ?	4
History and development of [*]	4
First use of [*] in a Warranted Context: [**]	6
4. Findings, Analysis, and Recommendations	10
[redacted] as a Novel Technology	10
Data Lifecycle Management	12
Risk Assessment Practices	13
Operational Technology Review Committee (OTRC)	15
Execution of Warranted Powers	16
[specific] Regulations	17
Duty of Candour	18
5. Conclusion	19
Annex A. Technical Inspection Report	20
Annex B. Lifecycle of [*]	25
Annex C. Findings and Recommendations	29

15(1)(f)

TOP SECRET // CEO

List of Acronyms

CSIS Canadian Security and Intelligence Service

DSE Designated Service Employee

[REDACTED]

[REDACTED]

IMSI International Mobile Subscriber Identity

IMVE Ideologically Motivated Violent Extremism

NSIRA National Security and Intelligence Review Agency

[REDACTED]

OTRC Operational Technology Review Committee

[REDACTED]

PSC Public Safety Canada

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Glossary of Terms

[specific] [redacted]	The regulations that govern [activities] in Canada, [redacted] [redacted]
Regulations [redacted]	[redacted]
[redacted]	[redacted]
IMSI catcher	A device used for intercepting mobile phone traffic and obtaining location data of mobile phone users.
Minister	In this report, Minister refers to the Minister of Public Safety and Emergency Preparedness.
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

TOP SECRET // CEO

Executive Summary

In this review, NSIRA examined the Canadian Security Intelligence Service's (CSIS's) lifecycle management of data collected pursuant to a Federal Court warrant. NSIRA's decision to undertake this review stems from its 2020 *Survey of CSIS's Technical Capabilities*.

In reviewing the activities of national security and intelligence federal departments and agencies, NSIRA assesses adherence to legal requirements, ministerial directions, policies, and internal procedures. In this case, NSIRA's broad conceptualization of "data lifecycle," which included the "how" of data collection, was intended to enable a comprehensive examination of CSIS's lawfulness and policy compliance.

While NSIRA observed professionalism and concern for lawfulness and policy compliance on the part of CSIS employees charged with the day-to-day operation and maintenance of the Service's operational and archival systems, it also found that inadequate planning and preparatory work on the part of other personnel undermines these employees' efforts at rigorous data stewardship.

Also concerning was CSIS's approach to its accountability and duty of candour obligations to the Minister of Public Safety and Federal Court, respectively. CSIS mischaracterized a novel technical capability as an extension of existing capabilities. As a consequence, CSIS did not consult Public Safety Canada about its plans to acquire this novel technical capability and did not notify the Public Safety Minister or the Federal Court prior to using it in an operation. Further, CSIS used this technology prior to satisfying all regulatory requirements.

1. Introduction

Authority

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

Scope of the Review

2. In this review, NSIRA examined the Canadian Security Intelligence Service's (CSIS's) lifecycle management of data collected pursuant to a Federal Court warrant. NSIRA's conceptualization of this lifecycle was deliberately broad, extending to the "how" of CSIS's data collection.
3. NSIRA's decision to undertake this review stems from its 2020 *Survey of CSIS's Technical Capabilities*¹ (Survey).
4. This review focused on CSIS's acquisition and use of [technology] [redacted] as well as its management of data collected using these [redacted] in a warranted [redacted] operation. NSIRA's assessment considered CSIS adherence to legal requirements, ministerial directions, policies, and internal procedures in its collection and stewardship of warranted data.
5. The period under review ranged from September 1, 2019 to August 15, 2023.

Methodology

6. To conduct this review, NSIRA analyzed documentation, received briefings, and attended onsite technical demonstrations delivered by CSIS subject matter experts. CSIS also provided direct access to many of the technical systems it uses to manage the lifecycle of warranted data. This direct access enabled NSIRA to independently search and examine many systems, identify novel avenues of inquiry, verify potential compliance issues, and validate information presented during briefings and demonstrations.
7. Given the many technical capabilities CSIS uses to collect warranted information, NSIRA developed assessment criteria to help sharpen its focus in this review. These assessment criteria—which ranked CSIS's technical capabilities according

¹ 20-09 Survey of CSIS's Technical Capabilities.

15(1)(f)

TOP SECRET // CEO

to maturity, complexity, sensitivity, and compliance considerations—led NSIRA to select the technical capability described in Section 6.

8. In creating its Inspection Method (see: Annex A), NSIRA engaged with national and international peer organizations.

Review Statements

9. Overall, CSIS partially met NSIRA's expectations for responsiveness on this review, as the quality of some responses and the Service's repeated lack of proactive disclosure did not meet NSIRA's expectations.
10. NSIRA was able to verify information received during the review in a manner that met its expectations and requirements. CSIS established a best practice for direct access. When engaging in discussions with NSIRA, CSIS personnel consistently offered frank and candid descriptions of systems, processes, and challenges. These open exchanges with CSIS personnel enriched the quality of this review.

2. Background

11. NSIRA's 2020 Survey documented numerous technologies, governance structures, and legal requirements that apply when CSIS uses technologies to support operations. The Survey concluded that NSIRA needed to remain current on the technical aspects of CSIS intelligence collection operations. Accordingly, this review examines the lifecycle of data collected under warrant—focusing on CSIS's first use of a novel technical capability in a [REDACTED] operation and its subsequent collection, assessment, ingestion, labeling, and archiving of data.
12. Technical capabilities are the sensitive tools and techniques CSIS uses to collect data that has intelligence value. For example, technical capabilities can be used to [REDACTED]
[REDACTED]
Technical capabilities are used in warranted and non-warranted contexts.
13. CSIS acquires technical capabilities in [REDACTED] ways: [REDACTED]
[REDACTED]
Of note, in a 2019 directive on accountability, the Minister instructed CSIS to consult the Deputy Minister of Public Safety Canada (PSC) about plans and proposals to seek a novel technique or technology.

15(1)(f)

TOP SECRET // CEO

14. To assist in its own consideration of novel technologies and techniques, CSIS recently established the Operational Technology Review Committee (OTRC).² When an operational team wants to develop or acquire a new technology, it is now required to present its proposal to the OTRC. The OTRC's role is to identify and assess potential risks attached to the procurement, development, testing and use of the new technology. To receive its full endorsement, the OTRC may recommend that CSIS notify the Minister and/or present the technology to the Federal Court to inform its decisions on warrant applications.
15. Warrant powers provide legal authorization for the use of sensitive tools, technologies, and/or techniques when their use would otherwise contravene Canadian law. In warrant applications, the affiant and Justice counsel are bound by the duty of candour which includes, among other things, providing adequate factual context and information concerning use of new intrusive techniques.
16. When using a new technical capability, CSIS personnel must follow internal operational procedures to ensure compliance with the Service's constitutional, statutory, Ministerial, Federal Court, and policy requirements. These procedures outline how to [REDACTED],³ [REDACTED],⁴ [REDACTED] for any [REDACTED] operation.
17. The procedures CSIS has established for assessing, ingesting, and storing data on its [REDACTED] operational and archival platforms—[REDACTED] outline the Service's approach to management of data collected under warrant. When CSIS uses a novel technology, it must prepare [platforms] to ingest [that which results from the novel technology] [REDACTED]

² Established in 2021, the OTRC is a senior management committee with representation from across CSIS.

³ [REDACTED]
[REDACTED]
⁴ [REDACTED]
[REDACTED]

15(1)(f)

TOP SECRET // CEO

18. According to Ministerial Direction and its own governance structure and policies, CSIS should follow the above processes every time it intends to study, acquire, or use a new technical capability to collect warranted data.
19. This review describes the lifecycle of warranted data collected by [*] a technical capability whose existence the Service twice failed to disclose. First, during NSIRA's 2020 *Survey of CSIS Technical Capabilities*, when NSIRA requested a list of current and anticipated technologies and, second, at the outset of this review when again asked.

3. [*] History, Development, and First Warranted Use

What is [*] ?

20. [*] is the designated technical capability codename for CSIS's

21. are unlike CSIS's other technical capabilities

[Technologies]

[Their use in Canada is regulated]

22. [Technical capabilities can capture sensitive information]

15(1)(f)

TOP SECRET // CEO

History and development of [REDACTED]

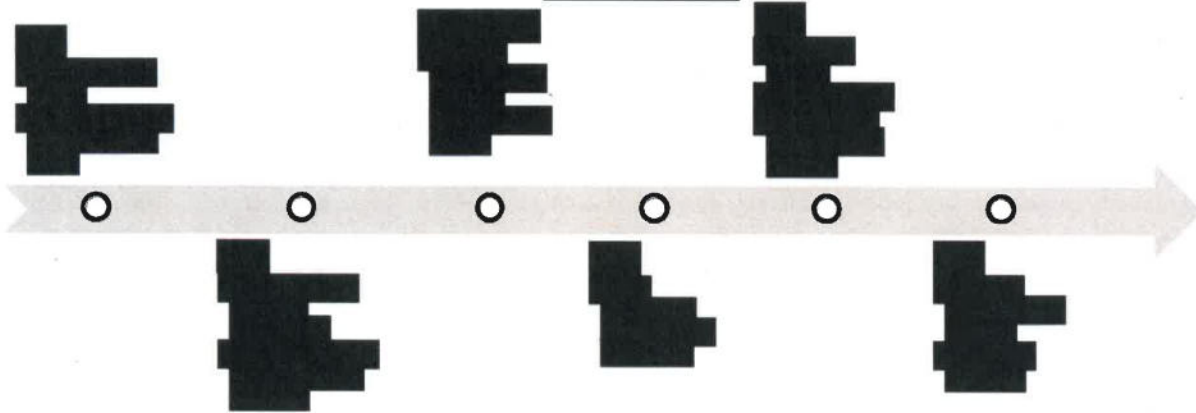


Figure 1: Timeline of CSIS's development and deployment of [REDACTED]

23. CSIS began exploring the potential operational use of [REDACTED] prior to 2017. In fact, by mid-2017, CSIS had started to centralize its [REDACTED] program under [project] [project] remains active as of September 2023 [...and contributes to technology development]
24. CSIS considered deploying [REDACTED] operationally as early as [REDACTED] 2018. At that time, personnel in [REDACTED] Region [REDACTED]
25. [REDACTED] CSIS did not

15(1)(f)

TOP SECRET // CEO

advise the Court of its [redacted] program, nor did it cease its efforts to deploy [redacted]
CSIS also did not engage or consult with PSC about [project] [redacted]

26. CSIS considered its next [redacted] deployment in [timeframe] . At that time, personnel
in [redacted] Region wanted to [apply technology] [redacted] While
planning the operation, [project member] [redacted]
[redacted] because the operation did not proceed.

27. [redacted]

28. In [timeframe] [redacted] [application of technology]
[redacted] in a non-warranted operation.
[The proposed operation had the potential to collect sensitive information].

29. CSIS considered another non-warranted [redacted] operation [location/time]
[redacted] It did not seek legal advice [redacted]
Because [redacted] CSIS abandoned the
operation.

First use of [*] [redacted] in a Warranted Context: [redacted]

30. In [target activity] [redacted]
[redacted] CSIS began

⁶ [target context] [redacted]

15(1)(f)

TOP SECRET // CEO

considering [application of technology]

16(1)(c)

[redacted] CSIS documents reveal that this operation was planned under a warranted authority.

31. On [timeframe] CSIS approved [*] operation [**]. In its approval documents, CSIS acknowledged that the relevant warrant [#] would expire in advance of the operation. CSIS noted [operational considerations] [redacted] that it would update its approval documentation once a new warrant was signed.

32. Also on [timeframe] Justice counsel and CSIS attended Court and sought a new [redacted] New warrants were issued, to take effect on [timeframe] The relied-upon warrant powers remained substantially the same.

33. The operation—[**]—became CSIS's first operational use of [technology] CSIS personnel participated in the planning and execution of [**] [redacted] the team did not seek legal advice [redacted] Moreover, CSIS informed neither the Federal Court nor PSC [redacted] prior to undertaking [**]

34. Despite being CSIS's first operational deployment of [technology] [redacted] assessed [redacted] as being [redacted] The basis for this assessment—which did not benefit from consultation with the Department of Justice or PSC on legal and reputational risks, respectively—[redacted] [** would make specific use of technology]

35. In its operational plan, [redacted] team stated that it planned to use [redacted] during the operation. Further, the plan indicated that the team would [redacted] [apply specific technology]

36. In [**] operational plan, CSIS also stated that it intended to [redacted] [collect information] [redacted] CSIS asserted that its authority to [collect sensitive information] was pursuant to the [redacted] Warrant, [redacted]

15(1)(f)

TOP SECRET // CEO

- [REDACTED]⁷ No legal advice was specifically sought in the planning of [REDACTED]
37. On [REDACTED] CSIS [REDACTED] executed [REDACTED] [REDACTED]
[REDACTED]⁸ The operational plan did not anticipate some of the foreseeable risks [REDACTED]
38. In the days following [REDACTED] [REDACTED] CSIS began identifying numerous issues as it attempted to assess, ingest, label, retain, and report on the data collected by [REDACTED]. Although [REDACTED] had been in development for years, CSIS had not considered how data would be [retrieved from technology] [REDACTED]. Consequently, no preparatory work to ingest [REDACTED] [REDACTED] data into [systems] [REDACTED] was undertaken. In the absence of this preparatory work, [operational] [REDACTED] staff decided to [REDACTED]. They provided [REDACTED] to [another team] [REDACTED] leaving its personnel to determine how to ingest [REDACTED] [REDACTED] data such that its lifecycle would be managed in a legally compliant manner. [REDACTED] personnel identified data duplication and lifecycle management risks associated with this unexpected process.
39. Throughout [REDACTED] managers worked on providing for the safe ingestion of [REDACTED] into [systems] [REDACTED]. They coordinated with other teams and confirmed that appropriate data labeling conventions would be in place. [REDACTED] employees sought to ensure that accurate data retention policies would be applied and that all metadata would reflect the correct collection date and time. However, despite these efforts, data labeling issues still arose once data was ingested and 'reported on'⁹ in [REDACTED]
40. While this data lifecycle management work unfolded, CSIS internally publicized [REDACTED] as its first successful warranted [REDACTED] operation in a [REDACTED] email. For many OTRC members, this internal email was how they learned of [REDACTED] [REDACTED] existence. Following discussion with management, the OTRC Chair agreed that [REDACTED] was a novel technology that should have been presented to and reviewed by the OTRC. Within days, CSIS paused all operational uses of [REDACTED] and tasked [REDACTED] [project] [REDACTED] to brief the OTRC.

⁷ CSIS planned [REDACTED] under the [REDACTED] warrant and executed it under the [REDACTED] warrant. In the [REDACTED] warrant, [REDACTED] The powers granted under [REDACTED] part remained substantively the same.

⁸ [REDACTED]

⁹ 'Reporting on' a product in [REDACTED] means that it has been included in an operational report for intelligence purposes.

15(1)(f)

TOP SECRET // CEO

41. By [redacted] were ready to ingest [redacted] data collected during [redacted]. A [redacted] Region employee reviewed and assessed all [redacted] opting to 'report on' [info] [redacted] and [info] [redacted] in [system] [redacted]. This changed the product's retention timeline from [redacted] to [redacted] days. The content of [redacted] and labeling applied to [sensitive information] [redacted] are described in Annex A.
42. During the summer of 2022, [redacted] [project] [redacted] members prepared their OTRC presentation and the OTRC Chair planned to notify PSC of CSIS's [redacted] program. When CSIS met with PSC on September 13, 2022, CSIS included [redacted] as part of a discussion about novel techniques and technologies. PSC disclosed that it was unaware of CSIS's [technology] [redacted] and that the technology seemed both novel and potentially controversial. PSC suggested that CSIS draft a memorandum for the Minister discussing novel technologies and techniques, including [redacted].
43. On September 26, 2022, [redacted] [project] [redacted] presented [redacted] to the OTRC. The presentation described [technology details] [redacted].
- ¹⁰ When identifying the legal authorities for conducting operations, the slide deck lists [specific] [redacted] Regulations and [redacted] Warrant, [redacted] [parts of warrant] [redacted] as being relevant. [redacted] [additional planning considerations] [redacted].
- [redacted]
44. On December 19, 2022, the OTRC "partially endorsed" CSIS's continued use of [redacted] in operations. The OTRC stated that CSIS "must present its past and prospective usage of [redacted] to the Federal Court in the context of an upcoming warrant application. The Court's reaction to this information will inform the scope of activities that can be carried out with and without a warrant." [redacted]

¹⁰ [applications of technology] [redacted]

15(1)(f)

TOP SECRET // CEO

- [redacted]
45. On [redacted] CSIS issued a Memo to the Minister notifying him that "since 2022, the Service has deployed [technology] [redacted] in support of s.12 warranted and non-warranted [operation type] operations on [#] separate occasions, and further operational uses are being contemplated."
46. On [redacted] CSIS notified the Federal Court in CSIS File [redacted] about its use of [redacted] as part of [redacted] affidavit focused on [redacted] [operation type] [redacted]

4. Findings, Analysis, and Recommendations

[redacted] as a Novel Technology

Finding 1. NSIRA found that [redacted] [technology] [redacted] are a novel technology within CSIS's suite of technical capabilities.

Finding 2. NSIRA found that [redacted] [technology] [redacted] introduce a significant expansion of collection capabilities and operational risks.

Finding 3. NSIRA found that CSIS does not have adequate policies and procedures to manage its [redacted] [technology] [redacted] program.

Finding 4. NSIRA found CSIS did not consult Public Safety Canada in a timely manner regarding its planned use of [redacted] [technology] [redacted], contrary to the *Ministerial Direction to the Canadian Security and Intelligence Service on Accountability* issued pursuant to section 6(2) of the CSIS Act. Moreover, CSIS may not be in compliance with section 7(1)(b) of the CSIS Act, which requires the Director to consult with the Deputy Minister when required pursuant to Ministerial Direction.

47. [redacted] are a unique tool in CSIS's suite of technical capabilities. [redacted]

[application of technology] [redacted]

Moreover, the [redacted]

-

15(1)(f)

TOP SECRET // CEO

52. CSIS technical staff decided—without seeking legal advice or guidance—to refer to [redacted] internally as [a type of operation] ¹¹ despite the differences between [redacted] and [redacted]. When questioned about this characterization, CSIS insisted that [redacted] are just [a type of operation]. This terminology obfuscates important distinctions between these two technologies, including [redacted] [specific technology application considerations] regulatory requirements for [redacted] and [redacted] system data flows.
53. A further consequence of considering [redacted] as [a type of operation] was that CSIS did not follow its internal procedures in advance of its first collection of [redacted] [*] data. This led to the delayed data ingestion and data labeling issues outlined in this report and in Annex A. CSIS failed to recognize the significant preparatory work required to ingest new data when deploying this novel technical capability.
54. Lastly, CSIS does not have current Standard Operating Procedures, a Concept of Operations, or a post-operational data clean up checklist for [redacted] [*]. These documents are crucial for ensuring that CSIS personnel execute [redacted] [*] and [redacted] [*] assisted operations in a compliant manner. NSIRA has previously documented CSIS's lack of current policies, and noted that its outdated policy suite may result in heightened compliance risks.

Recommendation 1. NSIRA recommends that CSIS establish and maintain adequate policies and procedures to manage its [redacted] [technology] program.

Data Lifecycle Management

Finding 5. NSIRA found that CSIS incorrectly labelled some data collected during [redacted] [***], and no quality assurance or compliance process detected this prior to NSIRA's technical inspection.

Finding 6. NSIRA found that CSIS retained collected information without clearly articulating the authority for its retention.

¹¹ [types of operations]
[redacted]

- Recommendation 2.** NSIRA recommends that CSIS prioritize investing in technical processes and systems that can assess, ingest, label, use, and destroy data in compliance with its legal obligations.

Finding 8. NSIRA found that CSIS relies on the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* to operationalize the 2019 *Ministerial Direction to the Canadian Security Intelligence Service on Accountability*. However, the 2020 *Framework* does not fully capture the requirements of the 2019 *Ministerial Direction*.

15(1)(f)

TOP SECRET // CEO

57. CSIS's consultation practices stray in significant ways from Ministerial Direction. For example, its current Framework agreement with PSC¹² does not reflect the Minister's stated desire to be consulted on the Service's plans to acquire novel technologies. The 2019 *Ministerial Direction to the Canadian Security Intelligence Service on Accountability* states that CSIS must consult with PSC on "[p]lans or proposals to use or seek a novel authority, technique or technology." *[emphasis added]*
58. Under the current Framework, this early consultation requirement is absent. Instead, the Framework only requires CSIS to inform PSC of its operational use of novel technologies. CSIS has taken the position that it will notify PSC about a novel technology only after it has obtained a legal opinion indicating that operational use of the technology poses a medium or high risk or when it is seeking a Federal Court warrant for an operation in which the technology figures. This is long after CSIS has [redacted] [considered] [redacted] the technology.
59. In examining CSIS's development and operational deployment [redacted] NSIRA saw instances where CSIS's lack of consultation with PSC and Justice resulted in CSIS employees unilaterally making policy and legal decisions. As a consequence, these decisions were taken without the appropriate departmental perspectives on questions of reputational and legal risk.
60. In the case of [redacted] [redacted] [redacted] CSIS only informed PSC about its new capability after using it, thus creating a *fait accompli*.
61. In addition, the criteria CSIS uses to identify novel techniques or technologies—criteria that form part of the Framework—are such that most technologies will not be considered novel, effectively precluding the Service from having to report anything to PSC.
62. This discrepancy between Ministerial Direction and current practice encroaches on the Minister's authority to make a policy intervention and undermines the Minister's ability to account for CSIS activities to Parliament.

Recommendation 3. NSIRA recommends that the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* be revised to fully align with the 2019 *Ministerial Direction to the Canadian Security Intelligence Service on Accountability*.

¹² See, for example, the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service*. This Framework sets out the particulars of the Service's engagement of PSC on risks arising from its activities.

TOP SECRET // CEO

Recommendation 4. NSIRA recommends that the definition of “novel technique or technology” in the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* be revised to err on the side of inclusivity.

Recommendation 5. NSIRA recommends that CSIS ensure risk assessments performed throughout the lifecycle of new technologies and techniques are rigorous, documented and comprehensive in their scope.

Operational Technology Review Committee (OTRC)

Finding 9. NSIRA found that the creation of the Operational Technology Review Committee was an important step forward in CSIS’s management of new technologies and techniques.

63. The OTRC identifies and assesses potential risks attached to the procurement, development, testing and use of new technologies and techniques. As such, the OTRC presents CSIS with an opportunity to engage PSC early on in its consideration of novel technologies and techniques. Were it to fully engage PSC in the OTRC’s deliberations, CSIS would be better aligning its practices with Ministerial Direction. CSIS documentation indicates that PSC has expressed a desire to attend or at least obtain the minutes of OTRC meetings. CSIS has thus far resisted these requests.
64. Not only does the OTRC represent a potentially important mechanism to engage PSC, it could also play an important role within CSIS, highlighting gaps in institutional collaboration; providing a mechanism to identify and consider the implications of novel technologies, including data lifecycle requirements; and exerting a measure of control over the Service’s deployment of novel technologies.
65. However, the OTRC remains a work in progress and efforts need to be made to ensure that all potential novel operational technologies and techniques fall under its scrutiny early on in their development. The fact that [**] took place prior to the OTRC even being briefed on the [REDACTED] program highlights the need to arrive at an agreed upon understanding of what constitutes a novel technology or technique.
66. More concerning is the OTRC’s lack of a rigorous and well-documented risk assessment process. Further, the relationship between the outputs of the OTRC’s process and those of CSIS’s operational risk assessment centre is unclear. These shortcomings have important implications. For example, when it identifies and assesses the potential risks of using new technologies or techniques in various

15(1)(f)

TOP SECRET // CEO

operational scenarios, the OTRC may determine that risk is elevated in one or more specific scenarios. Unless it documents and communicates this risk assessment to CSIS's operational risk assessment centre, the OTRC's review may be ineffective at preventing future operational failure or unlawfulness.

Recommendation 6. NSIRA recommends that, as part of its ongoing development, the Operational Technology Review Committee refine its processes to:

- consider data lifecycle requirements,
- reference a definition of 'novel technology' that has been agreed upon with Public Safety Canada as part of a revised Framework,
- include a requirement to consult Public Safety Canada on plans or proposals to seek or develop novel techniques and technologies,
- define how risk is assessed,
- better document its technical, legal, foreign policy and reputational risks assessments.

Execution of Warranted Powers

Finding 10. NSIRA found that, in [**], CSIS intended to [redacted]
[redacted] beyond warranted targets [at a location] [redacted]
[redacted]

67. At the [redacted] [#] warrant application hearing, the Service informed the Court that the purpose of [warrant] power in the warrant is to [redacted]. However, the warrant only authorizes the Service to [redacted] and to incidentally obtain [redacted]. CSIS's [redacted] planning documentation clearly indicated that [redacted] would be sought, and was not limited to the intention to only [redacted] with acknowledgement that [redacted] may be incidentally [redacted].
68. [CSIS retained [redacted] information on non-targets [redacted]] [redacted] There is some ambiguity as to whether [redacted] could be considered to have been incidentally obtained under the warrant. The warrant provisions should be amended to clearly delineate when CSIS has the authority to deliberately [redacted] [redacted]
69. The Service also acquired [redacted] as a result of the [redacted] operation. [Warrant type] [redacted]; the power to [redacted]

15(1)(f)

TOP SECRET // CEO

[excerpt from warrant type]

This power is limited, however, to
[certain types of sensitive information from targets]

There
is no provision to obtain information about
This power and its limitations were not considered during operation, where
planning documents indicated that
would be sought.

70. CSIS's execution of [warrant type] powers has implications beyond its use of [] as it applies to all [] under warranted powers. Clarity with respect to what [] and what is "incidental" would assist CSIS in ensuring that [] are obtained and retained in compliance with the law. Furthermore, if [] is used to execute the Service's warrant power to obtain information, the limits of this authority merit consideration.

Recommendation 7. NSIRA recommends that language in the [warrant type] [] Warrant more clearly describe the breadth and limitations of what constitutes incidental collection.

Recommendation 8. NSIRA recommends that CSIS specify the warrant authority in the operational planning documents in support of each type of [sensitive info] to be sought in the operation.

[Specific] Regulations

Finding 11. NSIRA found that CSIS's [use of technology] [] may not be in compliance with the [specific] Regulations.

71. [Specific] Regulations prohibit [certain applications of technology]

Regulations require [applicable regulatory requirement]

72. [] planning documents indicate that the team was aware that [] were not [configured in a specific way]
[] These documents do not raise the possibility that

15(1)(f)

TOP SECRET // CEO

[redacted] might be problematic, nor do they record any consultation with Justice as to whether this was permissible under [specific] Regulations.

73. When NSIRA questioned CSIS about this matter, CSIS responded that it had not [redacted] prior to operational use because [redacted] There is no provision in [specific] Regulations that permits [a certain application] Accordingly, [technology used in the course of **] [redacted] may not have been in compliance with [Regulations details] of [specific] Regulations.

Duty of Candour

Finding 12. NSIRA found that CSIS did not advise the Court prior to using [redacted] in the execution of warranted powers.

74. The *Policy of Justice and CSIS on the Duty of Candour in ex parte Proceedings*, which was in force at the time of the review and is a requirement of the 2019 *Ministerial Direction to the Canadian Security Intelligence Service on Accountability*, set out the respective responsibilities of both parties with respect to obligations to the Federal Court.¹³ Under this policy, both CSIS and Justice are required to undertake steps necessary to support and enable the discharge of the duty of candour by counsel and witnesses. The Policy specifically notes that the Court's discretion is informed by the broader context in which the warrant is issued. The intrusive capabilities of technical devices to be used in carrying out the warrant form part of this context. In particular, the Policy requires affiants to consider the need to provide information concerning the technical capacity of devices that would be used to execute a warrant. The policy sets out a similar requirement regarding the proposed use of a new intrusive technique. These requirements have not substantially changed under the updated 2023 policy.

75. [redacted]

¹³ An updated policy, OPS-1004: *Policy on the Duty of Candour in the Context of Judicial Authorizations under the CSIS Act*, effective September 8, 2023, replaced the 2017 *Policy of the Department of Justice Canada and the Canadian Security Intelligence Service on the Duty of Candour in ex parte Proceedings*. As the review period pre-dates the updated policy, NSIRA has reviewed [redacted] as it relates to the old policy.

15(1)(f)

TOP SECRET // CEO

[REDACTED] In its planning documentation, CSIS clearly intended to use a particular technology, [REDACTED] to execute [REDACTED]

76. CSIS approved [REDACTED] on the same day that CSIS was in Court seeking a new [REDACTED] warrant. The affidavit in support of the warrant describing the requested power consists of [REDACTED]
- [REDACTED] There was no discussion of the use of [REDACTED] in support of [warrant type] [REDACTED]. The Court was not informed of the planned use of [REDACTED] new intrusive technique, to execute these powers. CSIS should have advised the Court in a timely manner.

Recommendation 9. NSIRA recommends that the classified version of this report be shared with the Federal Court.

5. Conclusion

77. The Service's internal handling of [REDACTED] (*) and its warranted data raises concerns about how well prepared it is for the deployment of other novel technologies. The years-long arc of CSIS's [REDACTED] program is noteworthy due to the Service's inadequate engagement with key internal and external stakeholders. Despite the Ministerial Direction in 2019 requiring early consultation on CSIS's plans to seek novel technologies, CSIS failed to inform PSC and the Federal Court prior to using [REDACTED]. While the OTRC appears poised to address some of these issues within CSIS, it is less clear that the broader cultural changes needed to realize the OTRC's potential are underway. Until its organizational culture shifts from a narrow focus on data collection, under warrant or otherwise, to sound stewardship of data at every step of its lifecycle, CSIS will continue to place itself at risk of non-compliance with the law and Ministerial Direction.

- [illegible]

15(1)(f)

TOP SECRET // CEO

- [REDACTED]
- [REDACTED]
5. Although not cited in the planning documents, collection of [REDACTED] is authorized under [REDACTED] Warrant. The interpretation of this part [REDACTED] —results in the following ORs:
- [REDACTED]
- [REDACTED]
6. [Analysis systems were configured in certain ways to accept sensitive information in support of operation] [REDACTED]
- [REDACTED] The retention policy dictates how long retains data to meet [REDACTED] namely if it should be destroyed after [REDACTED] or not [REDACTED] defines reported data as that which has met the condition for retention and unreported data for that which has not.
7. [Analysis systems were configured to retain sensitive information in certain ways] [REDACTED]
- [REDACTED] This particular policy had a reported retention period of [REDACTED] and an unreported retention period of [REDACTED]
8. [REDACTED] were still active in [REDACTED] at the time of inspection, as opposed to [REDACTED] inactive. The associated investigative file [REDACTED] was also still active despite being associated to an expired court application and being configured with a warrant start date of [REDACTED] and end date of [REDACTED]
9. [REDACTED] collected a total of [REDACTED] and [REDACTED] as a result of [REDACTED]
- [REDACTED] All files were attributed to the [REDACTED]

15(1)(f)

TOP SECRET // CEO

investigative file [REDACTED] and to the target [REDACTED], matching those specified as part of the operational requirements.

10. [Analysis systems were configured to handle sensitive information A similarly to other types of information]
[REDACTED]
11. [Analysis systems were configured to handle sensitive information B similarly to other types of information]
[REDACTED]
12. [Analysis systems note important characteristics of sensitive information]
[REDACTED] This allows
to calculate the deletion time for each unique product it collects [REDACTED]
[in relation to warrant requirements]
[REDACTED]
13. The inspection of the available [REDACTED] for the [REDACTED] revealed that:
 - all were [REDACTED] on [REDACTED] between the hours [REDACTED] and [REDACTED]
 - [REDACTED] were imported on [REDACTED]
 - [REDACTED] were imported on [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - all had a deletion date of [REDACTED]
14. After the first inspection visit, NSIRA sought to verify the existence of [REDACTED] operational messages. CSIS confirmed that [REDACTED] did not exist and had erroneously been entered into [REDACTED]. At the second inspection visit, NSIRA observed that CSIS had corrected the operational message [REDACTED].
[REDACTED]
This confirmed CSIS's position that all [REDACTED] products were determined to assist in the investigation of a threat to the security of Canada and that CSIS no longer had to destroy them [REDACTED]

15(1)(f)

TOP SECRET // CEO

15. When [redacted] mark products as reported in [redacted] they are required by policy to enter [links to related information.] [redacted]

[redacted] The net result is a heightened risk of [redacted]
[redacted] [incorrectly assessing product] [redacted] retaining that
information under the reported retention period [redacted] without proper
justification.

16. [Sensitive information included unique properties generated by technology] [redacted]

[redacted] The collection of
[unique properties] as part of the collection of [sensitive info] is an
example of potential bycatch, namely the collection of additional information that
could risk conflicting with obligations or expectations between CSIS and the
Courts.

17. NSIRA examined [the consultations by certain officials of sensitive information
at location 1 and 2] [redacted]

18. [redacted]

19. [Analysis systems did not track certain interactions with information] [redacted]

20. NSIRA discovered [sensitive information from operation was linked with related
information] CSIS confirmed [redacted]

CSIS also stated that [redacted]

21. NSIRA reviewed [redacted] in [redacted] and observed that:

[redacted]

15(1)(f)

TOP SECRET // CEO

[REDACTED]

NSIRA was unable to determine if any of [REDACTED] included the intended target but was able to conclude that [REDACTED] definitely did not contain the target.

22. NSIRA reviewed all [REDACTED] in [REDACTED] and observed that:

[REDACTED]

NSIRA was unable to determine if any of [REDACTED] included the intended target but was able to conclude that at least multiple [REDACTED] and at least [REDACTED] did not contain the target.

23. [REDACTED] Such a statement, if intended to describe clearly does not meet the operational requirement to [REDACTED] or explain how [REDACTED] were assessed to be [REDACTED] the target [REDACTED]

24. Finally, although NSIRA was able to confirm [REDACTED] were archived for long term retention [REDACTED]

Annex B. Lifecycle of [* information]

1. This annex describes the technical systems involved with the Service's identification, collection, evaluation, retention, querying, exploitation, ingestion, and destruction of [* information]
2. The following description of the technical systems involved with the lifecycle of [* information] stems from CSIS briefings delivered on March 15, 2023, June 16, 2023, and July 11, 2023; a technical demo delivered on June 13, 2023; documentation received in response to NSIRA Requests for Information (RFIs); as well as technical inspections conducted on June 9 and July 28, 2023. This annex should be seen as reflective of the technical systems in place during the first operational use of [*]

CSIS's current [technology]

3. CSIS has previously [used older technology] and CSIS had not operational use.
4. [new technology]

Lifecycle of a [* information]

5. [CSIS uses * to collect information]
After the collection operation personnel review for quality control before transferring it to data collection system where it is catalogued and made available to data for intelligence analysis. This data is retained in data processing and management system where it is continuously evaluated for compliance (i.e., retained or destroyed according to pre-established timeframes informed by policy or warrant requirements).

15(1)(f)

TOP SECRET // CEO

Preparation

6. Before CSIS can collect and process data via [*]
[redacted] ensure the data can be collected, stored, manipulated, retrieved, retained, and destroyed properly.
[Information passes through different technologies.]
[redacted]
7. Prior to any [*] operation,
[CSIS conducts operational planning with technical considerations]
[redacted]
[redacted] With
respect to collecting data,
[redacted] however, this means CSIS
incidentally collects [redacted] other than the operational target(s).
[redacted]
8. Although [redacted] collection system had the capability to ingest data similar to
[other information]
[redacted] there were no formal preparations made to update
specifically for [redacted] data prior to [redacted] Rather, the [redacted]
introduced [redacted] specifically for
collection of [redacted] data in [redacted], approximately [redacted]
after [redacted] collected its data.

Collection and Triage

9. [CSIS used technology to collect information via **]
[redacted]
10. After [***] transfers data from [redacted]
[redacted] to [redacted] triage and

15(1)(f)

TOP SECRET // CEO

keep only what was relevant from the operation [REDACTED]
[REDACTED]. However, at this stage, [REDACTED] data is not evaluated for its intelligence value. [Data is deleted after being transferred]
[REDACTED]
[REDACTED]

Ingestion

11. Because [REDACTED] was not configured specifically to [REDACTED] data immediately following [REDACTED] data could not be ingested to directly. Instead, [REDACTED]
[REDACTED] [data was copied to a shared network]
[REDACTED] 4
12. On [REDACTED] and [REDACTED] ingested [REDACTED] and [REDACTED] from [REDACTED] respectively. [The data was organized based on its format.]
[REDACTED]
[REDACTED]

Processing and Analysis

13. Prior to [REDACTED] ingesting [REDACTED] data] [REDACTED] reviewed the [REDACTED] data on [REDACTED]
[REDACTED]. Once [REDACTED] data was eventually ingested to [REDACTED] later in [REDACTED] used [REDACTED] to determine [REDACTED] which inform how they can be retained before destruction.¹⁵ (This [REDACTED] also assists with [REDACTED]
[REDACTED] [enriching the data]
[REDACTED]

¹⁴ Following [REDACTED], CSIS has streamlined its procedures for transferring [REDACTED] data to [REDACTED] triage it, [REDACTED] ingests it [REDACTED]

¹⁵ [REDACTED]
[REDACTED]

15(1)(f)

TOP SECRET // CEO

Retention

14. [REDACTED] the data processing and management system which ingests, stores, and manages data from [REDACTED] evaluates data to ensure it remains compliant.

[** data retention period is influenced by its use]

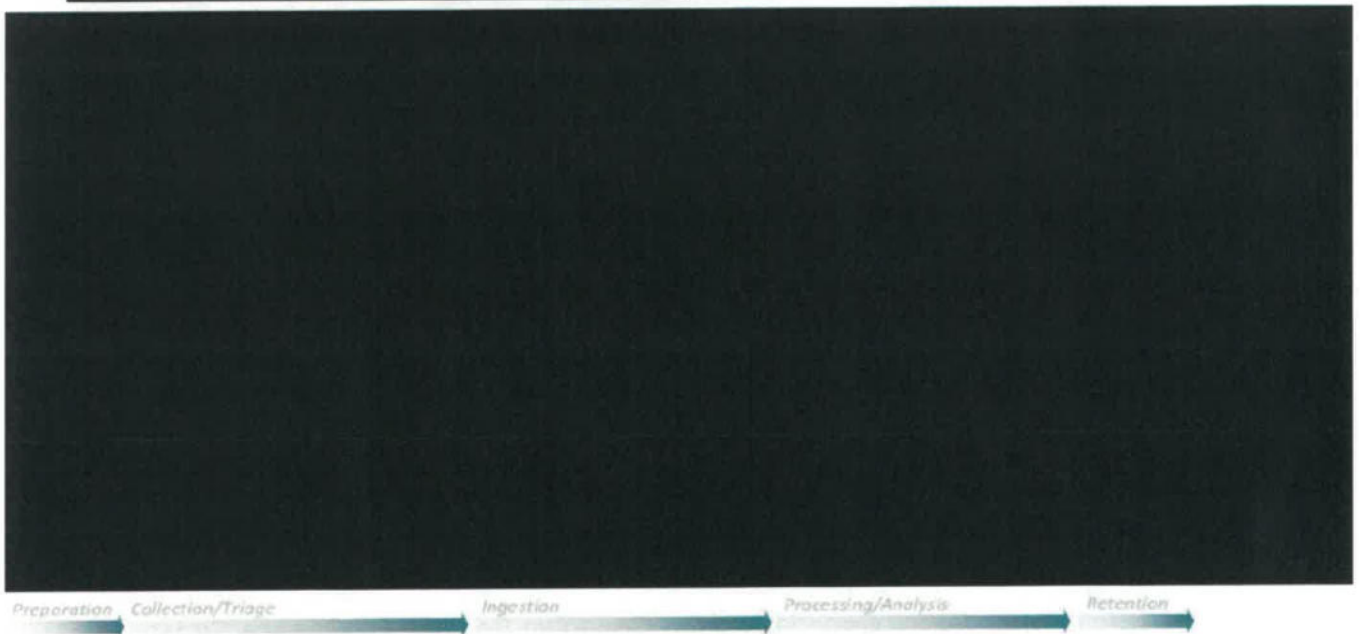


Figure 2 Dataflow for [**]

Annex C. Findings and Recommendations

NSIRA made the following findings and recommendations in this review:

Finding 1. NSIRA found that [technology] are a novel technology within CSIS's suite of technical capabilities.

Finding 2. NSIRA found that [technology] introduce a significant expansion of collection capabilities and operational risks.

Finding 3. NSIRA found that CSIS does not have adequate policies and procedures to manage its [technology] program.

Finding 4. NSIRA found CSIS did not consult Public Safety Canada in a timely manner regarding its planned use of [technology], contrary to the *Ministerial Direction to the Canadian Security and Intelligence Service on Accountability* issued pursuant to section 6(2) of the CSIS Act. Moreover, CSIS may not be in compliance with section 7(1)(b) of the CSIS Act, which requires the Director to consult with the Deputy Minister when required pursuant to Ministerial Direction.

Finding 5. NSIRA found that CSIS incorrectly labelled some data collected during [**] and no quality assurance or compliance process detected this prior to NSIRA's technical inspection.

Finding 6. NSIRA found that CSIS retained collected information without clearly articulating the authority for its retention.

Finding 7. NSIRA found that CSIS does not adequately consider data stewardship requirements accruing from new collection activities, which introduces heightened non-compliance risks.

Finding 8. NSIRA found that CSIS relies on the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* to operationalize the 2019 *Ministerial Direction to the Canadian Security Intelligence Service on Accountability*. However, the 2020 *Framework* does not fully capture the requirements of the 2019 *Ministerial Direction*.

Finding 9. NSIRA found that the creation of the Operational Technology Review Committee was an important step forward in CSIS's management of new technologies and techniques.

Finding 10. NSIRA found that, in [**] CSIS intended to [redacted] beyond warranted targets [at a location] [redacted]

15(1)(f)

TOP SECRET // CEO

Finding 11. NSIRA found that CSIS's [use of technology] may not be in compliance with [specific] Regulations.

Finding 12. NSIRA found that CSIS did not advise the Court prior to using [*] in the execution of warranted powers.

Recommendation 1. NSIRA recommends that CSIS establish and maintain adequate policies and procedures to manage its [technology] program.

Recommendation 2. NSIRA recommends that CSIS prioritize investing in technical processes and systems that can assess, ingest, label, use, and destroy data in compliance with its legal obligations.

Recommendation 3. NSIRA recommends that the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* be revised to fully align with the 2019 *Ministerial Direction to the Canadian Security Intelligence Service on Accountability*.

Recommendation 4. NSIRA recommends that the definition of "novel technique or technology" in the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* be revised to err on the side of inclusivity.

Recommendation 5. NSIRA recommends that CSIS ensure risk assessments performed throughout the lifecycle of new technologies and techniques are rigorous, documented and comprehensive in their scope.

Recommendation 6. NSIRA recommends that, as part of its ongoing development, the Operational Technology Review Committee refine its processes to:

- consider data lifecycle requirements,
- reference a definition of 'novel technology' that has been agreed upon with Public Safety Canada as part of a revised Framework,
- include a requirement to consult Public Safety Canada on plans or proposals to seek or develop novel techniques and technologies,
- define how risk is assessed,
- better document its technical, legal, foreign policy and reputational risks assessments.

Recommendation 7. NSIRA recommends that language in the [warrant type] Warrant more clearly describe the breadth and limitations of what constitutes incidental collection.

Recommendation 8. NSIRA recommends that CSIS specify the warrant authority in the operational planning documents in support of each type of [sensitive info] to be sought in the operation.

TOP SECRET // CEO

Recommendation 9. NSIRA recommends that the classified version of this report be shared with the Federal Court.