National Security and Intelligence Review Agency

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

Annual Review of Select Canadian Security Intelligence Service Activities, 2024

NSIRA // Review 23-12

Table of Contents

Glossary of Terms

Commission or Omission When a designated employee does or omits to do certain acts, under the specific conditions set in s. 20.1 of the CSIS Act that would otherwise constitute an offence.

Dataset Regime Sections 11.01 to 11.25 of the *Canadian Security Intelligence Service Act* governing datasets which defines a dataset as, "a collection of information that:

a) is characterized by a common subject matter;

b) is stored as an electronic record;

c) contains personal information, as defined in section 3 of the *Privacy Act*; and

d) is relevant to the performance of the Service's duties and functions under any of sections 12 to 16 but cannot be collected or retained under any of those sections".

Designated Employee An employee who performs information and intelligence collection activities and is designated under s. 20.1(6) or (8) of the CSIS Act, by the Minister of Public Safety and Emergency Preparedness or the Director in exigent circumstances, and may be justified in committing or directing another person to commit an act or omission that would otherwise constitute an offence.

Direction When designated employee who is authorized directs the commission of the act or omission that would otherwise constitute an offence under specific conditions set in s. 20.1(15) and (16) of the CSIS Act.

Evaluated Dataset A dataset which designated employees have evaluated no later than the 180th day after the day on which the dataset was collected and confirmed that the dataset:

- Was publicly available at the time of collection;
- Predominantly relates to individuals within Canada or Canadians and whether it belongs to an approved class; or
- Predominantly relates to individuals who are not Canadians and who are outside Canada or corporations

	that were not incorporated or continued under the laws of Canada and who are outside Canada.
Foreign Influenced Activities	Activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person.
Hostile State Actors	State actors that engage, either directly or via proxies, in actions that are deceptive, coercive, corruptive, covert, threatening or illegal, yet fall below the threshold of armed conflict, and which undermine Canada's national interests. These activities include conventional and well-known efforts, such as espionage and foreign interference, and other threats, such as disinformation, sabotage, the use of licit and illicit means to acquire intellectual property, economic coercion, and malicious cyber activities.
Intelligence Commissioner	The person appointed under the *Intelligence Commissioner Act* to review, among other duties, the conclusions on the basis of which certain authorizations are issued or amended under the CSIS Act.
Judicial Authorization	The process by which a Federal Court judge authorizes a specific actions, such as the retention of a Canadian dataset, search and seizure, or interception of private communications.
Justification Framework	Provides legal authority for CSIS employees who are specifically designated by the Minister of Public Safety, and persons acting under their direction, such as human sources, to engage in acts or omissions that would otherwise constitute offences.
Retained	A dataset that CSIS stores internally, subject to the appropriate authorization where necessary, for a specific period, or for future query or exploitation.
Security Assessments	An appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual for the purpose of government employment, or access to government sites.
Sequestering	Data that CSIS has secured, isolated, or removed for safekeeping to prevent its misuse or alteration.

Threats to the Security of Canada

a) Espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;

b) foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;

c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and

d) activities directed towards undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada;

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

Executive Summary

Through the CSIS Act, Parliament requires the Canadian Security Intelligence Service (CSIS) to provide the National Security and Intelligence Review Agency (NSIRA) with information related to seven categories of information. This report, the Annual Review of Select CSIS Activities 2024, examined a number of CSIS activities and operations that fall within these categories.

This review identified trends, gaps, and emerging issues. It analyzed CSIS's interpretation of its authorities and management of information. NSIRA traced broad themes in this review, including ensuring authority for activities and proper accountability to both the Minister and Canadians.

NSIRA used this review as an opportunity to follow-up on specific issues identified and recommendations made in previous reviews. For example, NSIRA conducted a technical inspection involving datasets and observed that CSIS had destroyed certain datasets as per a previous NSIRA recommendation.

NSIRA also observed that a longstanding concern remained an issue throughout 2024. CSIS may not be in compliance with the CSIS Act when it does not submit reports under s. 20(2) of the Act to Minister regarding potentially unlawful conduct by CSIS employees, including potential violations of the Charter. In 2025, the CSIS Director approved a memorandum to expand unlawful conduct reporting, NSIRA will continue to monitor this issue.

In another longstanding issue, NSIRA noted that CSIS has not implemented finalized procedures regarding financial intelligence collection and engagement with financial entities.

In 2024, CSIS sought and received a warrant to conduct a Threat Reduction Measure (TRM), marking its first use of this statutory authority. NSIRA recommended that CSIS develop a formal approval process for warranted TRMs.

NSIRA also reviewed how CSIS integrates the requirements of new Ministerial Directions into its policies. While NSIRA found that many policies had been updated, there remained gaps and NSIRA recommended that these be prioritized.

I. Introduction

Authority

1. This review was conducted pursuant to paragraph 8(1)(a) of the *National Security and Intelligence Review Agency Act* (NSIRA Act).
2. This review was also conducted pursuant to paragraph 8(2) of the NSIRA Act, which requires NSIRA to review at least one aspect of Canadian Security Intelligence Service's (CSIS) Threat Reduction Measure (TRM) performance; and paragraph 8(2.1)(a), requiring NSIRA to review the implementation of significant aspects of every new or modified ministerial direction issued to CSIS.

Scope of the Review

3. NSIRA reviewed select activities conducted by CSIS between January 1, 2024 and December 31, 2024.

Methodology

4. Each year, NSIRA completes an Annual Review of Select CSIS activities based on the information that CSIS must provide to NSIRA pursuant to the CSIS Act.[1] This flow of information gives NSIRA ongoing insight into CSIS activities.
5. In addition, NSIRA also requests supplemental information to enhance its understanding of the activities and allow for independent verification of the information provided. The supplemental information, which is critical to the execution of this review, includes internal compliance reporting, CSIS correspondence with Public Safety and the Federal Court, and Department of Justice opinions and advice to CSIS.
6. The review's analysis of select CSIS activities focuses on key compliance matters previously identified by NSIRA, especially those of particular relevance to the Canadian public. Particular attention was paid to novel powers, on-going non-compliance, increased risk, lack of sufficient accountability reporting and/or gaps in governance. Emerging issues identified as part of this review but not covered herein will support future review planning.

[1] See Annex A.

Review Statements

7. The NSIRA Act grants NSIRA rights of timely access to any information in the possession or under the control of a department (except for Cabinet Confidences) and to receive from the department any documents and explanations NSIRA deems necessary. NSIRA monitors cooperation with access requests, including the completeness and accuracy of disclosures, which informs its overall assessment of a department's responsiveness in each review.
8. CSIS partially met NSIRA's expectations for responsiveness during this review.

II. Background

9. Between 2019 and 2023, NSIRA undertook analysis to support its requirement to report annually to the Minister of Public Safety on CSIS Activities, resulting in classified accounts to the Minister further to s. 32 of the NSIRA Act. In addition to the 2024 classified report, NSIRA decided to align this work with its standard review practices and produce a report in accordance with s. 34 of the NSIRA Act.
10. The CSIS Act requires CSIS to provide NSIRA with information related to seven categories of activities:
    a) Threat Reduction Measures
    b) Datasets
    c) Unlawful Conduct
    d) CSIS Director's Annual Report to the Minister of Public Safety
    e) Ministerial Direction
    f) Justification Framework, and
    g) Domestic and Foreign Cooperation Arrangements.
11. These reporting requirements can be found in the CSIS Act, and are identified in detail in Annex A. NSIRA expects CSIS to provide this information in response to quarterly requests for information that detail specific documentation requirements. These requirements may extend beyond that which is explicitly outlined in the CSIS Act to ensure that NSIRA receives relevant information which can be assessed against the review objectives. NSIRA is confident that CSIS has provided all reporting required under the CSIS Act. NSIRA undertook spot checks using direct access to CSIS systems, and sought clarification and confirmation from CSIS as necessary.
12. There are nine discrete sections in this review. Seven of these address the categories of activities listed above, while two address other associated issues.

Each section contains available statistics related to the scope and breadth of CSIS operations, and displays the evolution of activities from year to year.

III. Findings, Analysis, and Recommendations

Section 1: Overview of CSIS Targets and Warrants

13. CSIS investigates threats to the security of Canada, including espionage, foreign influenced activities, political, religious or ideologically motivated violence, and subversion as defined in s. 2 of the CSIS Act. The CSIS Act sets out criteria permitting CSIS to investigate an individual, group, or entity for matters related to these threats. Subjects of a CSIS investigation, whether they be individuals or groups are called "targets".

Table 1: Total number of CSIS targets by year

	2019	2020	2021	2022	2023	2024
Number of Targets	467	360	352	340	323	389
Source: CSIS (NSIRA did not independently verify these numbers)						

14. Pursuant to s. 21 of the CSIS Act, CSIS makes an application to a judge for a warrant if it believes on reasonable grounds that more intrusive powers are required to investigate a particular threat to the security of Canada. Warranted powers may include intercepting communications, entering a location, or obtaining information, records or documents. Each warrant application could request multiple powers against different targets. While new warrants may be issued against new targets, 13 of 18 in 2024 (72%) of the current sample were new warrants against previously warranted investigations or targets. CSIS may apply for a supplemental warrant to add a new target to a warrant during the validity period.

Table 2: Warrant applications* and approvals, new, supplemental, or denied

	2019	2020	2021	2022	2023	2024
Total Warrant Applications	24	15	31	28	30	28
Total Warrants Issued by the Court	23	15	31	28	30	27
New Warrants	21	10	27	20	19	18
Supplemental	2	5	4	8	11	9
Total Denied Warrants	1	0	0	0	0	1
Source: CSIS (NSIRA did not independently verify these numbers) **Note: The warrant statistics found here represent the total number of warrant applications made to the Federal Court, independent of the actual number of**						

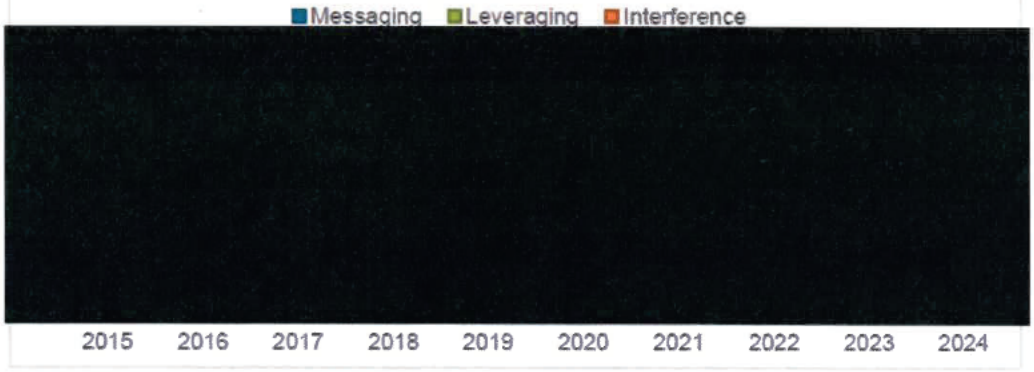
warrants granted in each application or the number of individuals who were the subject of warrants.

Section 2: Threat Reduction Measures (TRMs)

15. CSIS is authorized by s. 12.1 of the CSIS Act to take measures to reduce threats to the security of Canada, within or outside of Canada (Threat Reduction Measures, or TRMs).

16. CSIS TRMs can take the form of one of three broad categories of activity: messaging, leveraging, and interference. In general, messaging TRMs directly or indirectly push information to a threat actor or person impacted by the threat in an attempt to influence their behaviour or reduce the treat. Leveraging TRMs disclose information to a third party to enable them to take action, at their discretion, against the identified threat-related activities. Interference TRMs directly affect the ability of
15(1)(f) a threat actor to engage in threat related activity. Since 2019, [redacted] TRMs have been the most common type of TRM proposed by CSIS.

Figure 1: Number of Proposed TRMs by type
(Source: CSIS)



15(1)(a)

(NSIRA independently verified these numbers)

17. Through direct access, NSIRA confirmed that CSIS proposed [redacted] TRMs in 2024,
15(1)(a) ten of which were approved. The other approval in 2024 was for TRMs proposed in 2023; [redacted] and [redacted] remained in the approval process at the end of 2024.

18. TRMs approved in one year may be executed in future years. Seven TRMs approved in 2023 were executed in 2024. Operational reasons may also prevent an approved TRM from being executed. Accordingly, two TRMs that were approved in 2024 but not executed remain valid, one of which was executed in the first quarter of 2025.

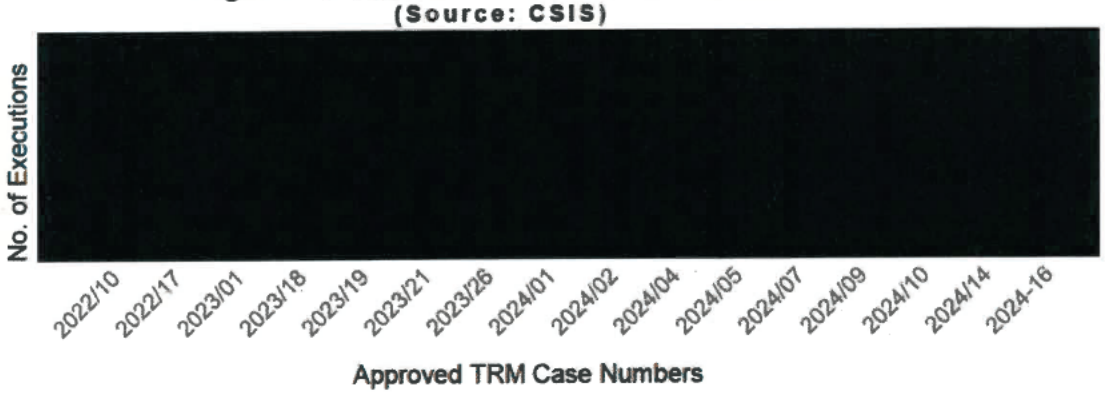
Table 3: Number of approved, executed, and warranted TRMs by year

	2019	2020	2021	2022	2023	2024
Approved TRMs	24	11	23	16	14	11
Executed TRMs	19	8	17	12	19	15
Warranted TRMs	0	0	0	0	0	1
Source: CSIS (NSIRA independently verified these numbers)						

19. A TRM may be executed multiple times during the approval period. The numbers in Table 3 (above) only capture whether the approved TRM was executed, and not the number of times it was executed. In 2024, CSIS conducted activities associated with fifteen approved TRMs a total of [redacted] times. [redacted] TRMs have some of the highest rates of execution, and have been used by CSIS consistently since 2015.

15(1)(a)

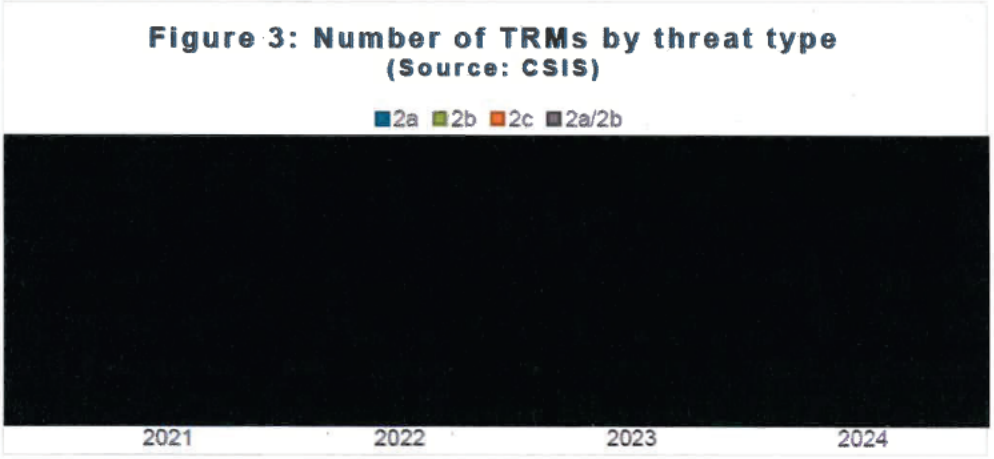
Figure 2: Number of TRM executions
(Source: CSIS)



(NSIRA did not independently verify these numbers)

20. NSIRA confirmed that over the last two years, [redacted] of executed TRMs were related to threats pertaining to s. 2(a) and 2(b) of the CSIS Act. TRMs in this area aim to reduce threats to Canadian security from hostile state actors. Such threats can include, among others, espionage, cyber attacks/operations, election interference, or transnational repression. This represents a considerable percentage increase when compared to 2021-2022 where only [redacted] of TRM activities were directed at these threats.

21. TRM activities targeting violent extremism (s. 2(c) threats) may have decreased in the last two years, however, CSIS has continued to target ideologically and religiously motivated violent extremism threat environment since 2015.



(NSIRA independently verified these numbers)

Warranted TRM

22. CSIS is required to seek a warrant for a TRM if it believes that certain intrusive measures, outlined in s. 21.1(1.1) of the CSIS Act, are required to reduce the threat. In 2024, CSIS obtained its first judicial authorization to undertake a warranted TRM.

23. Internally, CSIS proposed its first warranted TRM in 2015, but it was not approved for submission to the Federal Court. Two additional proposals, in 2018 and 2019 respectively, were also abandoned. These first three proposed TRMs focussed on the threat posed by violent extremism. Since then, the rate at which warranted TRMs were proposed and considered has increased. The prevalence of [redacted] proposals since 2022 is noteworthy: [redacted] proposed warranted TRMs were [redacted]

(Source: CSIS; NSIRA independently verified these numbers.)

24. In 2024, CSIS sought and obtained judicial authorization for its first warranted TRM. As part of this review, NSIRA focused on the process CSIS followed to obtain the warrant. NSIRA did not review the specifics of the execution of the warranted powers, rather initiated a dedicated review to examine this TRM in greater detail.

Finding 1. NSIRA found that CSIS lacks a formal and documented process for warranted Threat Reduction Measure (TRM) approvals, creating delays in the consideration and approval of these proposals that may affect viability of the TRM itself.

25. It has been nine years since the CSIS Act was amended to allow for threat disruption powers including the authority for a TRM warrant. NSIRA expected that CSIS would have a formal and documented warranted TRM approval process in place. Instead, NSIRA saw that while a draft warranted TRM workflow had been created, it was never finalized. This workflow outlined the steps necessary to obtain operational approval for a warranted TRM proposal, prior to commencing the steps required to obtain judicial authorization. CSIS reported that the total anticipated time for the warranted TRM approval process was 4-6 months, not including the time required to seek judicial authorization.

26. Processing times and the lack of procedures for warranted TRM applications have prevented some employees from submitting proposals. Consequently, delays in the internal approval process and necessary external consultation may also lead to missed opportunities to reduce threats.

27. In the absence of a specific process, for the first warranted TRM CSIS attempted to follow its standard (collection warrant) prioritization and approval process, despite procedural differences in these activities.

Recommendation 1. NSIRA recommends that CSIS institute a formal approval process for warranted threat reduction measure proposals that accounts for timelines for external consultations.

Section 3: Datasets

28. Further to the *National Security Act, 2017*, the CSIS Act was modified to include s. 11.01-11.25 which enables CSIS to collect and use datasets to support its duties and functions. It also establishes safeguards for the protection of Canadian rights and freedoms, including privacy rights. These protections include enhanced requirements for ministerial accountability. Depending on the type of dataset, CSIS must meet different requirements before it is able to use a dataset. In 2024, Bill C-70 made further amendments, including changes to the definition of a dataset, lengthening the time for evaluations, Intelligence Commissioner Authorizations, and Judicial Authorizations.

29. Within CSIS, the dataset regime is now referred to as the dataset authority, and CSIS policies are in the process of being updated to reflect the 2024 legislative amendments.

Table 4: Number of datasets newly evaluated and retained by year

	2019	2020	2021	2022	2023	2024
Publicly Available Datasets						
Evaluated	9	6	4	4	2	2
Retained	9	6	2	4	2	2
Canadian Datasets						
Evaluated	0	0	2	0	1	0
Retained	0	0	0	2	0	0
Foreign Datasets						
Evaluated	10	0	0	2	1	2
Retained	0	1	1	1	3	4

Source: CSIS (NSIRA did not independently verify this information).
Note: Datasets collected and evaluated in one year, may receive Ministerial, Judicial, or other authorization in subsequent years. Datasets may be retained for multiple years as per the CSIS Act.

Finding 2. NSIRA found that CSIS is at risk of collecting information that is publicly available, but for which there may be a reasonable expectation of privacy, as was noted in NSIRA's Review of CSIS Dataset Regime (21-15).

30. In NSIRA's Review of CSIS Dataset Regime 21-15 ("Dataset Review"), NSIRA highlighted that while the CSIS dataset policy does codify the commitment to not collect stolen, hacked or leaked datasets, there is no corresponding requirement to ensure that information contained in publicly available datasets does not contain information for which there is a reasonable expectation of privacy. The review also highlights that while the dataset policy guides employees on the dataset regime, it places the onus on "employees who collect the dataset" to determine the appropriate collection authority.

"Referential Datasets"

31. Prior to the coming into force of the *National Security Act, 2017*, CSIS reviewed its data catalogue to prepare for the implementation of the new dataset regime. The focus was on datasets containing personal information; subject to the new legal authority requirements under the CSIS Act. A class of datasets that CSIS calls "referential datasets" were not included in this review as they were deemed out of scope at the time, as they did not fall within the definition of a dataset as per s. 11.02 of the CSIS Act. According to CSIS, "referential datasets" are publicly

available on the internet and do not contain personal information, examples include geographic names, maps, Statistics Canada data, Internet Protocol (IP) addresses, and area codes.

32. In January 2024, the Supreme Court of Canada released its decision in *R. v. Bykovets,* which found that there is a reasonable expectation of privacy attached to an IP address.

33. CSIS has issued an *Interim Directive on the Non-warranted Collection of IP Addresses* which states that as a result of the Bykovets decision, CSIS's collection of IP addresses under the CSIS Act "**may** engage s. 8 Charter rights and warranted authorities **may** now be required for collection activities that were previously unwarranted" (emphasis added). [redacted]

34. While the Bykovets decision has provided clarity from the Supreme Court on the reasonable expectation of privacy associated with IP addresses, CSIS awaits decisions from the Federal Court to further understand the full extent of its impact on CSIS investigative, collection, and analytical activities.

35. When NSIRA asked if CSIS held datasets requiring reassessment following the Bykovets decision, CSIS advised that it does not maintain a list of "referential datasets", as these types of datasets are widely available and easily accessible on the Internet. According to CSIS, these types of datasets do not contain personal information, and are not subject to legal consideration under the CSIS Act. As such, CSIS is of the opinion that its employees may obtain and use "referential datasets" as needed for their work.

36. At the same time, CSIS provided a list of several "referential datasets" available on the CSIS internal open source portal, noting these as an exception to the rule. According to CSIS, these select "referential datasets" were brought in and made available on the portal as a convenience to all employees, eliminating the need to log into external Internet accounts to access information.

37. In the Dataset Review, NSIRA recommended that CSIS meaningfully analyze and document any possible reasonable expectations of privacy when evaluating publicly available datasets. CSIS partially accepted NSIRA's recommendation stating that the template used to evaluate datasets includes a prompt for the designated employees to include comment and assessment regarding personal information and reasonable expectations of privacy.

Recommendation 2. NSIRA recommends that CSIS evaluate all its publicly available and "referential" datasets for the presence of information which may attract a reasonable expectation of privacy, and that this evaluation be conducted by employees with the necessary expertise.

Dataset Retention: Technical Verification Exercise

Finding 3. NSIRA confirmed that CSIS destroyed datasets that were no longer strictly necessary to retain as per Recommendation 7 in NSIRA's Review of CSIS Dataset Regime (21-15).

38. NSIRA sought to independently verify the steps taken by CSIS in response to the following recommendation from the Dataset Review:

> NSIRA recommends that CSIS immediately destroy Canadian and foreign dataset information that is not strictly necessary to retain. This information no longer falls within the legal 90 day evaluation period and retaining it pursuant to the dataset regime is no longer a possibility.

39. As part of the verification exercise, NSIRA sought to determine whether CSIS had destroyed these datasets, which NSIRA had found to be unlawfully retained. NSIRA also sought to confirm that files related to the datasets and identified operational messages were destroyed.

40. NSIRA conducted a technical verification exercise to determine if CSIS had addressed previously-issued recommendations. This verification included demonstrations and direct access to CSIS systems. NSIRA verified that the requested datasets and operational messages were no longer present, retrievable, or accessible in the systems that were available to NSIRA (see Annex B).

Section 4: Compliance

41. CSIS's internal operational compliance program is the centre for processing all instances of potential non-compliance related to operational activities. The unit manages the reporting and assessment of potential non-compliance incidents against CSIS authorities in order to provide advice and guidance related to the operational community to prevent recurrence of non-compliant activity.

Table 5: Number of instances of potential non-compliance and violations

Incidents	2019	2020	2021	2022	2023	2024
Processed Incidents						
Administrative	-	53	64	42	48	54
Operational[2]	40[3]	19	21	17	31	28
Total	53	99	85	59	79	82
Breakdown of Non-compliance (all categories counted)						
Canadian Law	-	-	1	2	4	5
CSIS Act	-	-	-	-	-	3
Charter	-	-	6	5	15	14
Warrant Conditions	-	-	6	3	11	13
CSIS Governance	-	-	8	15	27	25
Source: CSIS (NSIRA did not independently verify these numbers)						

42. NSIRA reviewed all incidents of potential non-compliance finalized in 2024. NSIRA expected that CSIS's process for reporting potential instances of non-compliance would not only identify, but also lead to actions taken by CSIS to address and resolve non-compliant activities.

43. CSIS required extended timelines to complete determination assessments, with nine incidents remaining unresolved for more than 500 business days and dating back to 2021. For one incident in particular, CSIS finalized the incident assessment report more than 700 business days after being initially notified of the incident. The level of severity of these incidents ranges from potential non-compliance with internal policies and procedures to a breach of warrant authorities, potential breach of Charter rights, and high legal risks of being contrary to the CSIS Act. CSIS communicated to NSIRA that there is currently no policy requirement to complete fact finding reports with a certain timeframe.

44. In the case study below, NSIRA highlights how unresolved incidents of non-compliance create a risk of recurrence.

---

[2] For 2021, each operational non-compliance incident was reported based on the highest non-compliance (i.e. if the incident were non-compliant with the Charter and CSIS governance, it would be counted only under the Charter category). For 2022 and 2023, each incident is counted in all of the areas in which it was noncompliant. As such, the sum of operational non-compliance in the various categories exceeds the total number of such incidents.

[3] The total number of incidents of non-compliance were not further broken down in 2019 and 2020. This number represents the number of incidents of non-compliance with requirements such as the CSIS Act, the Charter, warrant terms and conditions, or CSIS internal policies or procedures.

Disclosures from Financial Institutions: Compliance Case Study

45. In 2024, CSIS continued to receive information from financial institutions provided pursuant to disclosure obligations under the *Criminal Code* regarding terrorist owned or controlled property and disclosure permitted under the *Personal Information Protection and Electronic Documents Act* in certain circumstances, including national security related information. In this review, NSIRA did not examine the information itself, including whether it fit within the financial institution's disclosing authority and/or whether it is strictly necessary to collect pursuant to CSIS's mandate. CSIS' centre for operational compliance has reviewed these disclosures and produced a report detailing concerns.

46. Currently, CSIS is sequestering the information and reminding financial institutions to stop providing specific personal information. Similarly, CSIS has been developing a set of standard operating procedures regarding financial intelligence collection and engagement with financial entities. This guidance has been in draft form since August 2023 and NSIRA has not observed any permanent solution to address this concern. NSIRA will monitor this issue and may initiate further review.

Section 5: Reporting Unlawful Conduct

Finding 4. NSIRA found that CSIS may not have acted in compliance with the law when it failed to submit reports to the Minister under s. 20(2) of the CSIS Act regarding potentially unlawful conduct by CSIS employees, including potential violations of the *Canadian Charter of Rights and Freedoms*.

47. Pursuant to s. 20(2) of the CSIS Act, if the Director of CSIS is of the opinion that an employee may have acted unlawfully while performing their duties and functions, the Director shall report the incident to the Minister of Public Safety. The Minister is then required to send a copy of the report to the Attorney General of Canada and NSIRA. Reporting unlawful conduct to the Minister is a fundamental accountability mechanism in the CSIS Act.

48. CSIS has consistently interpreted its s. 20(2) responsibility as requiring the Director to report to the Minister only incidents that, in the Director's opinion, could constitute a prosecutable offence. As part of this review, NSIRA requested all documents related to disclosures to the Minister under s. 20(2) of the CSIS Act. NSIRA was provided documentation related to three occasions where memorandums were sent to the Minister further to this requirement since 2017:

15(1)(d)

- [redacted]

- [redacted]
- [redacted]

49. Although CSIS does include a list of unlawful activity in an appendix in the Director's Annual Report to the Minister of Public Safety, this listing does not provide sufficient detail to allow the Minister to understand the context of the unlawful activity or to assess its severity. The Director's 2023-2024 Annual Report included a list of 22 instances of non-compliance with the Charter. While NSIRA expected to see that all instances of potentially unlawful conduct, including *Charter* violations, reported to the Minister pursuant to s. 20(2) of the CSIS Act, none have been reported. NSIRA considers that this may constitute a non compliance with the law.

50. NSIRA's concerns about CSIS's approach to this reporting requirement are longstanding, a position that NSIRA most recently articulated in its 2023 Classified Annual Report to the Minister of Public Safety. In March 2025, the Director of CSIS approved a memorandum endorsing an interpretation of the reporting requirements under s. 20(2) that includes actions or operational activities that violate Charter rights or lack statutory authority, regardless of whether the activities constitute a prosecutable offence.

51. NSIRA expects to see implementation of the reporting required by s. 20(2) in 2025 and will continue to monitor this issue.

Recommendation 3. NSIRA recommends CSIS trigger the application of section 20(2) of the CSIS Act in relation to potentially unlawful conduct by CSIS employees, including potential violations of the *Canadian Charter of Rights and Freedoms*.

Section 6: Director's Report

Finding 5. NSIRA found that there was insufficient attention dedicated to significant legal issues within the Director's Annual Report to the Minister of Public Safety.

52. The CSIS Act requires the Director to submit an annual report to the Minister of Public Safety with respect to CSIS's operational activities, and to provide a copy to NSIRA. CSIS met these requirements in 2024.

53. The Ministerial Direction on Accountability (2019), specifies an additional list of requirements for inclusion in the annual report. NSIRA confirmed that the report met most of these requirements, but did not explicitly and adequately reflect the extent of the legal issues facing CSIS and the efforts undertaken to address them.

Absent a dedicated section, such legal issues and efforts to address them risk not being given the prominence they merit.

Recommendation 4. NSIRA recommends that CSIS explicitly and adequately report on significant legal issues facing CSIS and efforts undertaken to address them in the Director's Annual Report to the Minister on CSIS Activities, as set out in the *Ministerial Direction on Accountability*.

New Government Security Screening Initiative

Finding 6. NSIRA found that CSIS introduces risks of stereotyping non-Canadian security clearance applicants from identified countries by issuing special country briefs in their security clearance assessment detailing generalized threat-related activities of the foreign government with no connection to the applicant besides their citizenship.

54. The Director's Annual Report included a section on security screening which contained details of a new security screening initiative launched by CSIS.

55. CSIS provides security assessments to Government of Canada client departments on individuals seeking security clearances for the purposes of government employment. Departments rely on this information in determining whether to grant or deny a security clearance to the individual in question. Security assessments, completed pursuant to s. 13 of the CSIS Act and the *Standard on Security Screening* (SSS) under the *Policy on Government Security*, are "an appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability ***of an individual***" [emphasis added]. In assessing reliability as it relates to loyalty, CSIS may consider whether:

> ...personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties to persons living in countries that pose a security risk to Canada, the individual has acted, is acting, may act or may be induced to act in a way that constitutes a threat to the security of Canada; or the individual has disclosed, may disclose, may be induced to disclose, or may cause to be disclosed in an unauthorized way, sensitive information.

56. In 2023-2024, CSIS began to include a "Non-Canadian Citizen Brief" (NCCB) as part of their security assessment when a security screening candidate is a citizen of certain enumerated countries, *and* not a Canadian citizen. The NCCB is included regardless of whether any adverse information was found specific to the security screening candidate. CSIS equates citizenship of the enumerated country as an "association with persons or groups considered to be a security threat" as outlined in the SSS.

57. Integrated into the person's security assessment, the brief is not bespoke to the individual. It contains threat-related information about the country with the individual's citizenship being the only connection between the individual and the country. No further information or analysis is included to tailor the information to the individual security-screening applicant.

58. CSIS's initial justification for launching this initiative was that citizens of China could be compelled, pursuant to China's national intelligence law, to provide information to that government. Despite the country specific nature of the law, CSIS has expanded the program, and includes the NCCB in security assessments related to citizens from other countries for which no similar laws have been cited.

59. While the brief states that the "[CSIS] has not identified specific adverse or threat-related information regarding the subject", they continue that the individual "may be at risk of being induced to cooperate with a hostile foreign state in a way that constitutes a threat to the security of Canada". CSIS highlights the risks to Canada of a compromise of sensitive information and includes a warning to the department:

> Should your department choose to assume the risk of granting a security clearance to [country name] national who does not possess Canadian citizenship, you may wish to consider implementation of a security waiver and any mitigation measures, as appropriate, pursuant to s. 13, appendix D of the SSS.

60. When asked how many non-Canadian citizens currently hold Canadian government security clearances, CSIS advised that the granting of security clearances is done by departments, not CSIS. Departments are responsible for informing CSIS of their clearance decisions, yet according to CSIS, many do not report back. As such, CSIS does not have readily available and reliable statistics as to how many non-Canadian citizens hold Canadian government security clearances. Furthermore, at this point, CSIS does not know whether departments in receipt of security assessments containing an NCCB are approving clearances, and if so, whether they are following CSIS's advice to implement security waivers or mitigation measures. Although this may be a function of delays inherent in the security screening process, CSIS also advised NSIRA that departments are not regularly reporting back to them with their decisions regarding screening.

61. The updated *Directive on Security Screening* (January 2025) now restricts non-Canadian citizens from obtaining Top Secret or Enhanced Top Secret clearances. There is no similar prohibition against non-citizens obtaining Secret or Site-Access clearances. As such, the observations in this section continue to be relevant as they apply to these individuals.

Section 7: Ministerial Direction

Finding 7. NSIRA found that certain CSIS policies and procedures do not fully align with the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians* and the *Ministerial Direction for Operations*.

62. In 2023, the Minister of Public Safety and Emergency Preparedness issued two new ministerial directions to CSIS: The *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians* and the *Ministerial Direction for Operations*. CSIS's timeliness with revising policies and procedures is critical to ensuring compliance with ministerial direction.

63. NSIRA examined 19 relevant policies and procedures for alignment with the two new ministerial directions. NSIRA noted 13 policies were updated in 2024. As of January 2025, six remained in the review process with completion targeted for 2025-2026, of which four had already received some updates in 2024. Policies related to conduct of operations, warrants, human sources, dangerous operating environments, cooperation with foreign partners, and security advice and assessments, are among those awaiting alignment.

64. The ministerial directions also impact the *Framework for Cooperation between CSIS and Public Safety* (the "Framework"). Despite the requirement that the two parties "review the Framework when a new ministerial direction is issued, or an existing ministerial direction is revised, or every three years" it has not been revised since 2020, and does not reflect the two new MDs issued in 2023, nor one MD issued in 2019.

65. Sections missing from the Framework include ministerial notification of high-risk operational activities inside and outside of Canada, the use of employees of federal organizations as human sources, CSIS employees discharging firearms in the course of duty, high-risk threat reduction measures, and foreign and domestic arrangements. Also missing is the requirement of the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians* that CSIS is to inform the Minister of all instances of threats to the security of Canada directed at Parliament and parliamentarians in a timely manner with an explanation of how CSIS will implement the direction.

66. In addition to the two MDs discussed above, in NSIRA's *Review of the Lifecycle of CSIS's Warranted Information*, NSIRA recommended that the Framework be aligned with requirements of the *Ministerial Direction on Accountability*. This recommendation remains un-actioned. Given its importance, it is reiterated within this review.

Recommendation 5. NSIRA recommends that CSIS:

a) prioritize updating its governance and policies to align with Ministerial Directions, and

b) collaborate with Public Safety to prioritize updating the *2020 Framework for Cooperation with Public Safety Canada and the Canadian Security Intelligence Service*.

The Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians: Case Study

Finding 8. NSIRA found that select operational activities carried out pursuant to the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*, did not meet all the requirements of the governance protocol supporting the Ministerial Direction.

67. In May 2023, the *Ministerial Direction on Threats to the Security of Canada directed at Parliament and Parliamentarians* was issued. This MD requires CSIS, wherever possible, to ensure that Parliamentarians are informed of threats to the security of Canada directed at them.

68. In September 2023, the Minister approved a governance protocol for threat disclosures to Parliamentarians whenever CSIS assesses that there is threat to the security of Canada directed at a Parliamentarian. It identifies that disclosure of the information to the Parliamentarian is legally possible while protecting the security and integrity of national security and intelligence operations and investigations. This protocol guidance includes several high-level consultations, and accountability measures, required documentation, as well as a detailed guide for undertaking associated operational activities.

69. At the time, the CSIS Act included restrictions on information sharing leaving CSIS to conduct classified threat briefings to Parliamentarians pursuant to its threat reduction mandate. The 2024 amendments to the CSIS Act have provided CSIS with more options with regard to information sharing.

70. NSIRA examined documentation associated with a high-risk TRM in which CSIS provided classified threat briefings to several former and current Members of Parliament in response to threat related activities undertaken by a foreign state and proxies. This TRM was undertaken in relation to the ministerial direction and required Ministerial approval.

71. NSIRA found that the briefings largely followed the governance protocol, however, there were certain deviations. One briefing that was delegated to a Parliamentary

staff member to perform did not include all necessary documentation required by the protocol.

Recommendation 6. NSIRA recommends that CSIS follow the governance protocol approved by the Minister in taking actions pursuant to the *Ministerial Direction on Threats to the Security of Canada directed at Parliament and Parliamentarians*.

Section 8: Justification Framework

72. The *National Security Act, 2017* created a limited justification framework for CSIS designated employees, and persons acting at their direction, to commit acts or omissions that would otherwise constitute offences under Canadian law. CSIS's Justification Framework provided needed clarity as to what CSIS may lawfully do in the course of its activities. It recognizes that it is in the public interest to ensure that CSIS employees can effectively carry out intelligence collection duties and functions, including by engaging in acts or omissions that would otherwise constitute offences, in accordance with the rule of law.

73. At least once every year, the Minister determines the classes of acts and omissions that would otherwise constitute offences that designated CSIS employees may be justified in committing or directing another person to commit. These must be approved by the Intelligence Commissioner. Employees must meet a reasonableness and proportionality test in order to be justified in committing an act or omission themselves (commissions by employees), while in order to direct another person to commit an act or omission (directions to commit), an employee must be authorized to do so by the Director or a Senior Designated Employee. The CSIS Act sets out clear limitations on this framework. For example, the Justification Framework does not permit acts or omissions that would infringe a right or freedom guaranteed by the Charter.

Table 6: Total number of authorizations, commissions, and directions under the JF (2019-2024)

	2019	2020	2021	2022	2023	2024
Commissions by Employees	1	39	51	61	47	34
Authorizations	49	147	178	172	172	175
Directions to Commit	15	84	116	131	116	128
Emergency Designations	0	0	0	0	0	0
Source: CSIS (NSIRA independently verified these numbers)						

74. In 2019, the Intelligence Commissioner approved seven classes of acts or omissions justified under the framework. In 2022, the Intelligence Commissioner

approved an eighth class. Classes are valid for a one-year period from the date the determination is approved by the Intelligence Commissioner.

75. CSIS activities aimed at the threat posed by [redacted] continue to dominate the use of the Justification Framework. In 2024, 110 of the 128 (86%) of the directions related to these threats.

76. With the exception of the first two years of the program, the number of authorizations has remained stable. The number of directions is consistently lower, as not all authorizations are used each year. In 2023, there were more than 90 authorizations for which there were no directions to commit, but this number was reduced to 70 in 2024. In 2023, approximately 10 authorizations, first authorized in 15(1)(d) 2021, with no related directions ended. In 2024, more than a dozen such authorizations remained.

77. In 2024, there was a marked increase in the number of authorizations, directions, and commissions related to CSIS's [redacted] mandate [redacted]. This type of authorization was first noted in 2021, with one authorization, one direction, and no commissions that year. Following which, there were no further authorizations, directions, or commissions made pursuant to [redacted] until 2024.

78. NSIRA is currently conducting a separate review of the Justification Framework.

Section 9: Cooperation Arrangements (S. 17)

79. CSIS's authority to enter into arrangements with foreign states, or an institution thereof, other government departments, police departments, and governments of the provinces is derived from s. 17 of the CSIS Act and requires the approval of the Minister of Public Safety and, in the case of foreign arrangements, consultation with the Minister of Foreign Affairs. A copy of any new or modified arrangement must be provided to NSIRA. As of June 2024, CSIS maintains more than 300 arrangements in more than 150 countries/territories.

IV. Conclusion

80. Through legislation, Parliament set out specific categories of information and activities for NSIRA to review. Based on this, NSIRA selected specific activities within these categories that warrant additional scrutiny. This report makes findings that speak to the current state of affairs at CSIS, and makes recommendations to CSIS to improve processes, prioritize accountability, protect privacy interests, and comply with the law.

81. The intent of this report was to provide a high-level overview of CSIS activities with deeper analysis as required. It is necessarily broad in nature, and does not include an in-depth examination of every issue NSIRA encountered. NSIRA may conduct future targeted reviews based on the information received, and it will continue to monitor areas of concern.

82. The issues reviewed here go to the heart of CSIS's authorities and examine how these authorities trigger accountability obligations to the Minister and ultimately to Canadians.

Annex A. Reporting Requirements and Responses

The following chart captures the reporting requirements for CSIS and identifies what NSIRA expects to receive in response. The chart also sets out what NSIRA actually received from CSIS in response to these reporting requirements. It does not capture information provided by CSIS in response to follow-up requests for information, briefings, or access which may have been required by NSIRA as part of this review.

Requirements under the CSIS Act	Expected by NSIRA in 2024	Received by NSIRA in 2024
Ministerial Direction		
The Minister may issue to the Director written directions with respect to the Service and a copy of any such direction shall, forthwith after it is issued, be given to the Review Agency.	Copies of directions issued by the Minister of Public Safety to the Director of CSIS.	Copy of *Ministerial Direction on Operations*. Copy of *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians* and associated guidelines document.
Director's Report		
The Director shall, in relation to every 12-month period or any lesser period that is specified by the Minister, submit to the Minister, at any times that the Minister specifies, a report with respect to the Service's operational activities during that period, and shall cause the Review Agency to be given a copy of each such report.	A copy of the Director's annual report to the Minister.	A copy of the Director's annual report to the Minister, including detailed references supporting the content in the report.

Requirements under the CSIS Act	Expected by NSIRA in 2024	Received by NSIRA in 2024
Datasets		
The Service shall given the Review Agency any report prepared with respect to publicly available datasets, verifying if the results obtained from the query and exploitation of those datasets were retained in accordance with sections 12 to 16 of the CSIS Act.	Copies of verification reports concerning the retention of results obtained from querying or exploiting a publicly available dataset, or querying, exploiting, or retraining a Canadian or foreign dataset.	Verification reports
In the case of a foreign dataset authorized as per the CSIS Act and that has been approved by the Intelligence Commissioner, notify the Review Agency when the Service removes information related to Canadians and of the measures that have been taken in respect to that information.	A notification of information relating to a Canadian or person in Canada having been removed from a foreign dataset as authorized by the Intelligence Commissioner or any measure taken concerning this information.	Notification of destruction of Canadian information.
In the case of a query of a dataset performed on the basis of exigent circumstances as per the CSIS Act, give the Review Agency a copy of the Director's authorization under that section and indicate the results of the query and any actions taken after obtaining those results.	Copies of Director's authorizations to query a Canadian or foreign dataset in exigent circumstances, as well as a report identifying the results of the query and any action taken.	Lists of new and / or renewed datasets and ingestion and retention dates. List of queries and exploitations of Canadian and Foreign datasets.

Requirements under the CSIS Act	Expected by NSIRA in 2024	Received by NSIRA in 2024
Threat Reduction Measures		
The Service shall, after taking measures, within or outside Canada, to reduce a threat, notify the Review Agency of the measure as soon as the circumstances permit.	Copies of tracking reports identifying all approved and implemented measures, with associated status updates.	Copy of the TRM tracking report, updated quarterly.
Domestic & International Cooperation Arrangements		
Where a written arrangement is entered into for the purpose of performing its duties and functions under the CSIS Act, a copy thereof shall be given forthwith to the Review Agency.	Copies of arrangements entered into by CSIS and another entity, and any associated Department of Justice written legal opinions, or briefings materials provided to Public Safety.	Documents related to various arrangements
Unlawful Conduct		
If the Director is of the opinion that an employee may, on a particular occasion, have acted unlawfully in the purported performance of the duties and functions of the Service under the CSIS Act, the Director shall cause to be submitted a report in respect thereof to the Minister. The Minister shall cause to be given to the Attorney General of Canada a copy of any report that he receives, together with any comment that he considers appropriate. A copy of anything given to the Attorney General of Canada	Copies of any report submitted to the Minister concerning unlawful conduct of CSIS employees, and any associated Department of Justice written legal opinions.	None

Requirements under the CSIS Act	Expected by NSIRA in 2024	Received by NSIRA in 2024
shall be given forthwith to the Review Agency.		
Justification Framework		
The Service shall notify the Review Agency as soon as the circumstances permit after a) designation is made of an employee who performs information and intelligence collection activities to be justified in committing or directing another person to commit an act or omission that would otherwise constitute an offence; b) an authorization is given to a designated employee to direct another person to commit an act or omission; and c) a written report submitted by a designated employee who committed an act or omission or who directed the commission of an act or omission.	Copies of designations. Copies of authorizations to direct the commission of acts or omissions. Copies of written reports submitted regarding the commission of an act or omission or the direction to commit an act or omission.	Notification Chart containing name, message number and date for each of the designations, authorization and commissions.
Supplemental Information		
Compliance		
None	Internal compliance reporting	Fact-finding reports related to potential non-compliance.
	Copies of any findings or non-compliance including fact	Determinations reports related to

Requirements under the CSIS Act	Expected by NSIRA in 2024	Received by NSIRA in 2024
	finding reports and final determination reports in relation to any activities undertaken by CSIS including administration, governance, processes and operations.	potential non-compliance.
	Copies of compliance incident trackers covering the period under review.	Copies of CSIS Compliance Tracker.
	Executive Committee on Compliance and Enforcement transcripts, meeting minutes and Records of Decision covering the review period.	Documents related to compliance cases.
Audit and Evaluation plans and reports		
None	Final audit and evaluation reports related to mandated activities, including governance, processes and operations.	Departmental audit and evaluation plans. Final Reports related to various completed audits and evaluations.
Federal Court Correspondence		
None	Copies of classified decisions. Copies of initial correspondence with the Court regarding CSIS warrants as well as copies of follow-up reports and correspondence including but not limited to cover letters, updates and notifications.	Various

Requirements under the CSIS Act	Expected by NSIRA in 2024	Received by NSIRA in 2024
	Copies of correspondence with the Court regarding compliance incidents. Copies of correspondence with the Court regarding the interpretation of the law in relation to CSIS or that relate to how CSIS conducts its activities.	
Legal Opinions & Advice		
None	Department of Justice written assessments, advice or opinions with respect to CSIS's legal obligations or protections, pertaining to governance, processes and operations specifically those which are: a) Foundational in nature, b) Establish frameworks c) Relate to new or novel activities, or, d) Changes in position.	[redacted]
Quarterly Engagement with Public Safety		
None	Copies of quarterly briefing material to Public Safety. Copies of associated speaking notes. Copies of the record of decision.	Copies of quarterly presentations. Copies of records of decision. Copies of speaking notes.

23

Annex B. Dataset Retention Technical Verification Exercise

1. Between January 29, and February 6 2024, NSIRA conducted a number of technical verifications, details of which are discussed below.

Table A: CSIS information a previous NSIRA review recommended for destruction

15(1)(d)

Type	Source	Title
[redacted]		

Source: NSIRA Review 21-15

2. To make a determination of CSIS's destruction requirement, NSIRA first identified which systems CSIS used to collect, evaluate, and retain information. After consulting with CSIS, NSIRA identified [redacted] systems, depicted in Figure A.

15(1)(d)

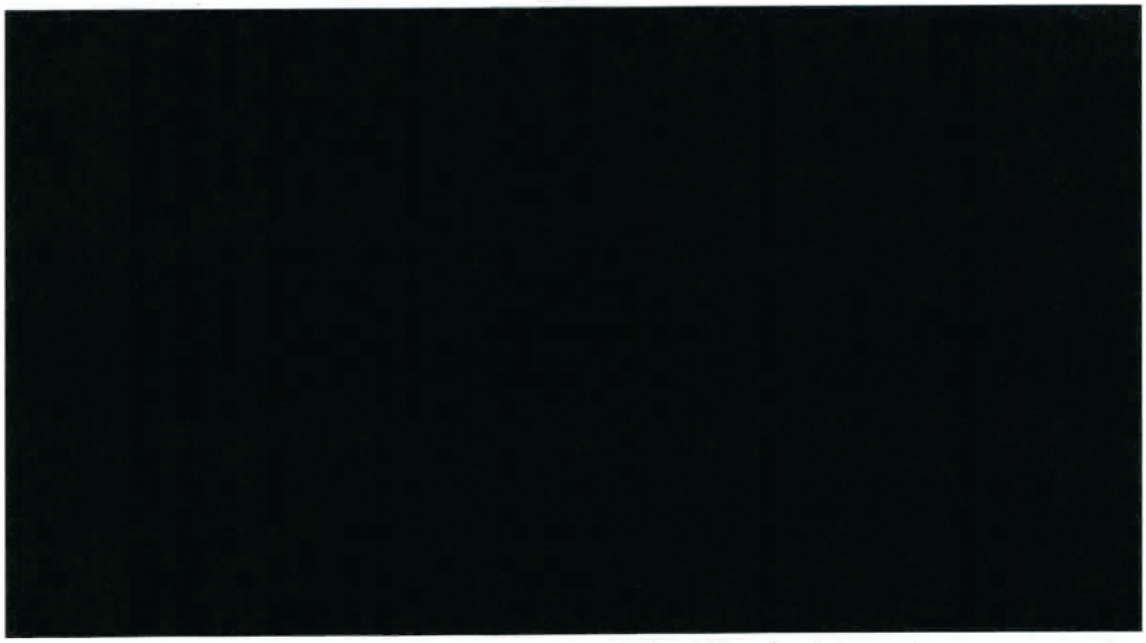


Figure A: Select dataset components and relationships

3. Due to the variety of underlying technologies CSIS used to manage data, NSIRA took a multi-faceted approach to independently verify whether the dataset information was no longer available. Where it had direct access to CSIS systems, NSIRA sought to verify that CSIS met the destruction requirements. In the other cases, NSIRA relied on CSIS expert personnel to leverage their broad access and execute custom queries, and to then provide documentary evidence of the results. NSIRA notes, however, that limitations on system access permissions could have affected query results.

4. On January 29, 2025, NSIRA accessed [redacted] to search for any record matching the titles from the collection of information. Additionally, NSIRA searched for each file's original unique record identifier it had previously recorded. In all cases, none of the original files were present.

5. Also on January 29, 2025, NSIRA accessed [redacted] to search for the [redacted] identified CSIS Operational Messages. While neither original message was available, there were many others that referenced them. Of note, all referenced messages were authored on or before 2019 (i.e. when the dataset regime came into force) except for one which was authored on [redacted]

6. On January 31, 2025, NSIRA used direct access to the [redacted] to search for the existence of any files related to the four identified datasets [redacted] For these datasets, CSIS had used the [redacted] to import them in preparation for evaluation. To track the import and evaluation process, CSIS's [redacted] team created [redacted] issues for each dataset. As per CSIS instruction, the [redacted] is intended to store each file (or dataset) as transitory information while it is being ingested [redacted] where it will eventually be evaluated. Further, each file is meant to be saved under a folder that corresponds to the datasets [redacted] issue [redacted] Regardless, a full search of the [redacted] was performed and revealed no files related to any of the four datasets.

7. Also on January 31, 2025, NSIRA directly accessed [redacted] to review the issues used in the management of the four datasets. Strangely, each dataset had a corresponding issue that had been duplicated and closed in 2023 with no

[redacted]

15(1)

15(1)(f)

additional detail. In addition, NSIRA was unable to retrieve any of the duplicated issues with the system, finding that the issues were either deleted or unavailable due to access limitations.

8. On February 6, 2025, NSIRA met with CSIS expert personnel and conducted a series of tests in an effort to determine if elements of any of the four datasets remained on operational systems. Queries via the CSIS employee's access revealed that NSIRA was missing a special system permission preventing access to certain [redacted] issues, including those related to the destruction tracking of the four datasets. At NSIRA's direction, the CSIS employee queried [redacted] directly using all available title permutations and identified tracking numbers. Additional searches for the same criteria in CSIS's custom search platform [redacted] which pulls its results from both the [redacted] All queries returned no results.

9. Also on February 6, 2025, NSIRA sought to retrieve and review any audit log messages specific to the deletion of the four datasets. However, CSIS confirmed that such messages are not generated following the removal of any dataset tables created within [redacted] for evaluation purposes.

10. Finally, NSIRA observed an April 18, 2023 email from CSIS's Deputy Director of Operations ordering the destruction of the four datasets. Internal responses confirmed that the datasets were destroyed from [redacted] on April 25, 2023, from the [redacted] on April 27, 2023, and from [redacted] on May 9, 2023. These actions correspond with what was documented in the reviewed tracking issues and further corroborated by NSIRA's technical verification exercise.

Annex C. Findings and Recommendations

NSIRA made the following findings and recommendations in this review:

Section 2: Threat Reduction Measures (TRMs)

Warranted TRM

Finding 1. NSIRA found that CSIS lacks a formal and documented process for warranted Threat Reduction Measure (TRM) approvals, creating delays in the consideration and approval of these proposals that may affect viability of the TRM itself.

Recommendation 1. NSIRA recommends that CSIS institute a formal approval process for warranted threat reduction measure proposals that accounts for timelines for external consultations.

Section 3: Datasets

Finding 2. NSIRA found that CSIS is at risk of collecting information that is publicly available, but for which there may be a reasonable expectation of privacy, as was noted in NSIRA's Review of CSIS Dataset Regime (21-15).

"Referential Datasets"

Recommendation 2. NSIRA recommends that CSIS evaluate all its publicly available and "referential" datasets for the presence of information which may attract a reasonable expectation of privacy, and that this evaluation be conducted by employees with the necessary expertise.

Dataset Retention: Technical Verification Exercise

Finding 3. NSIRA confirmed that CSIS destroyed datasets that were no longer strictly necessary to retain as per Recommendation 7 in NSIRA's Review of CSIS Dataset Regime (21-15).

Section 5: Reporting Unlawful Conduct

Finding 4. NSIRA found that CSIS may not have acted in compliance with the law when it failed to submit reports to the Minister under s. 20(2) of the CSIS Act regarding potentially unlawful conduct by CSIS employees, including potential violations of the *Canadian Charter of Rights and Freedoms*.

Recommendation 3. NSIRA recommends CSIS trigger the application of section 20(2) of the CSIS Act in relation to potentially unlawful conduct by CSIS employees, including potential violations of the *Canadian Charter of Rights and Freedoms*.

Section 6: Director's Report

Finding 5. NSIRA found that there was insufficient attention dedicated to significant legal issues within the Director's Annual Report to the Minister of Public Safety.

Recommendation 4. NSIRA recommends that CSIS explicitly and adequately report on significant legal issues facing CSIS and efforts undertaken to address them in the Director's Annual Report to the Minister on CSIS Activities, as set out in the *Ministerial Direction on Accountability*.

New Government Security Screening Initiative

Finding 6. NSIRA found that CSIS introduces risks of stereotyping non-Canadian security clearance applicants from identified countries by issuing special country briefs in their security clearance assessment detailing generalized threat-related activities of the foreign government with no connection to the applicant besides their citizenship.

Section 7: Ministerial Direction

Finding 7. NSIRA found that certain CSIS policies and procedures do not fully align with the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians* and the *Ministerial Direction for Operations*.

Recommendation 5. NSIRA recommends that CSIS:

a) prioritize updating its governance and policies to align with Ministerial Directions, and

b) collaborate with Public Safety to prioritize updating the *2020 Framework for Cooperation with Public Safety Canada and the Canadian Security Intelligence Service*.

The Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians: Case Study

Finding 8. NSIRA found that select operational activities carried out pursuant to the *Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians*, did not meet all the requirements of the governance protocol supporting the Ministerial Direction.

Recommendation 6. NSIRA recommends that CSIS follow the governance protocol approved by the Minister in taking actions pursuant to the *Ministerial Direction on Threats to the Security of Canada directed at Parliament and Parliamentarians*.