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

REVIEW OF CSIS THREAT REDUCTION MEASURES

NSIRA // Review 2022 - 04

TOP SECRET // CEO // SOLI-CLI

Table of Contents

EXECUTIVE SUMMARY

1. (U) This review is the third annual review of Canadian Security Intelligence Service (CSIS) threat reduction measures (TRMs) completed by the National Security Intelligence Review Agency (NSIRA).

2. (U) The review had two main objectives. First, to provide an overview of TRMs in 2021, contextualizing the data as appropriate by comparison with data from preceding years and noting any trends or patterns that emerge. Second, to conduct a review of a selection of TRMs implemented in 2021.

3. (S) NSIRA found that CSIS's use of its TRM mandate in 2021 was broadly consistent with its use in preceding years. Overall, CSIS implemented [redacted] TRMs during the review period, covering a range of threats to the security of Canada (as defined by section 2 of the *CSIS Act*), including espionage/sabotage, foreign interference, and violence/terrorism. Of note, 2021 marks the first time since the inception of the regime that TRMs involving Ideologically Motivated Violent Extremism (IMVE) threats outnumbered those stemming from Religiously Motivated Violent Extremism (RMVE).

15(1)(d)(ii)

4. (S) In terms of trends over time, NSIRA observed that the year 2018 was an inflection point for CSIS's use of the TRM mandate. In that year, CSIS proposed nearly as many TRMs as were proposed in the preceding three years – the first three of the mandate – combined. In the following year, however, the number dropped slightly, before a more significant reduction in 2020. This downward trend plateaued during the review period, even rebounding gently. The number of proposed TRMs in 2021 went up as compared to the previous year, as did both approvals and implementations.

5. (U) NSIRA selected three TRMs implemented in 2021 for review, assessing the measures for compliance with applicable law, ministerial direction, and policy. At the same time, NSIRA considered the implementation of each measure, including the alignment between what was proposed and what occurred and, relatedly, the role of legal risk assessments for guiding CSIS activity, as well as the documentation of outcomes.

6. (U) For all the cases reviewed, NSIRA found that CSIS met its obligations under the law, specifically the *Canadian Charter of Rights and Freedoms* and sections 12.1 and 12.2 of the *CSIS Act*. In addition to general legal compliance, NSIRA found that CSIS sufficiently established a "rational link" between the proposed measure and the identified threat.

7. (U) For one of the three cases reviewed, NSIRA found that CSIS did not meet its obligations under the 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* issued by the Minister of Public Safety.

8. (S) The TRM in question [redacted] NSIRA believes that the presence of these factors ought to have factored into the overall risk assessment of the measure. [redacted] In addition, however, are the risks [redacted] These risks are not, and in this instance were not, captured by CSIS's reputational risk assessment.

15(1)(d)(ii)

9. (S) Similarly, the legal risk assessment for this TRM did not comply with the ministerial direction that "legal risk is to be assessed in accordance with the Department of Justice risk criteria." [redacted] Under CSIS's "TRM Modernization" project, implemented in January 2021, [redacted] NSIRA recommended that LRAs be conducted for TRMs [redacted] and, further, that CSIS consider and evaluate whether legal risk assessments under TRM Modernization comply with applicable ministerial direction. NSIRA may revisit this issue – and TRM Modernization as a whole – in a future review.

23

10. (U) A comparative analysis of the two LRAs provided for the other TRMs under review underscored the practical utility of clear and specific legal direction for CSIS personnel. Clear direction allows investigators to be aware of, and understand, the legal parameters within which they can operate and, subsequently, allows after-action reporting to document how implementation stayed within said bounds.

11. (U) With respect to documenting outcomes, NSIRA further noted issues with, and made recommendations for, when CSIS produces certain reports following implementation of a TRM. Specifically, NSIRA recommended specifying in policy when the Intended Outcome Report and Strategic Impact Report are required. While cognizant that overly burdensome documentation requirements can unduly inhibit CSIS activities, NSIRA nonetheless believes that the recommendations provided are prudent and reasonable. Relevant information, available in a timely manner, benefits CSIS operations.

12. (U) NSIRA review is an important part of the TRM regime. The *CSIS Act* requires CSIS to notify NSIRA after it has implemented a TRM, while the *NSIRA Act* requires NSIRA to review, each calendar year, at least one aspect of CSIS's performance in undertaking TRMs. The result is enhanced likelihood that CSIS will use the TRM mandate lawfully and responsibly. In this vein, it bears underscoring the general finding of compliance – with law, ministerial direction, and policy – at the core of this review, noted issues notwithstanding.

13. (U) NSIRA employees directly and independently accessed the relevant CSIS database to review and verify information. Following an initial analysis, follow up Requests for Information (RFIs) targeted specific documents identified as missing or potentially relevant. NSIRA shared a preliminary draft of the report with CSIS to verify its factual accuracy. NSIRA has high confidence in the information it examined in the course of this review, and consequently in the findings and recommendations emerging therefrom.

List of Figures

List of Tables

List of Acronyms

[redacted] 15(1)(d)(ii)

CSIS – Canadian Security Intelligence Service

IMVE – Ideologically Motivated Violent Extremism

LRA – Legal Risk Assessment

MD – Ministerial Direction

NSIRA – National Security and Intelligence Review Agency

ORA – Overall Risk Assessment

RCMP – Royal Canadian Mounted Police

RFA – Request for Approval

RFI – Request for Information

RGB – Reasonable Grounds to Believe

RGS – Reasonable Grounds to Suspect

RMVE – Religiously Motivated Violent Extremism

SIRC – Security and Intelligence Review Committee

TRM – Threat Reduction Measure

AUTHORITIES

14. (U) This review was conducted under the authority of subsection 8(2) of the *National Security and Intelligence Review Agency Act* (*NSIRA Act*).[1]

INTRODUCTION

Background

15. (U) This review is the third annual review of CSIS threat reduction measures (TRMs) completed by the National Security Intelligence Review Agency (NSIRA). NSIRA's predecessor, the Security Intelligence Review Committee (SIRC), examined CSIS's use of threat reduction measures between 2016 and 2019.

16. (U) NSIRA review is an important part of the TRM regime.[2] The *CSIS Act* requires CSIS to notify NSIRA after it has implemented a TRM, while the *NSIRA Act* requires NSIRA to review, each calendar year, at least one aspect of CSIS's performance in undertaking TRMs. In this way, the significant power conferred by the creation of the TRM mandate in 2015 is countervailed by regular and rigorous independent review.

17. (U) NSIRA's 2020 Review examined a sample of TRMs to assess their compliance with law, policy, and ministerial direction. The review found that, in a limited number of cases, individuals were included in a TRM without a rational link between the individual and the identified threat. Relatedly, NSIRA cautioned that overly broad rational link criteria could affect a measure's reasonableness and proportionality. The review also noted that more consideration was needed with respect to the possible existence of an agency relationship between CSIS and third parties receiving information from CSIS.[3]

18. (S) NSIRA's 2021 Review focused on the latter dynamic, examining cases involving the disclosure of information from CSIS to external parties with their own levers of control and the extent to which CSIS appropriately identified, documented and considered any plausible adverse impacts such measures could have on individuals. The review made recommendations in these areas, including that CSIS "comply with its record-keeping policies related to documenting the outcomes of TRMs."[4]

---

[1] *National Security and Intelligence Review Agency Act*, SC 2019, c 13, s 2.
[2] For a summary of the TRM mandate, see Annex B.
[3] NSIRA, *Review of CSIS Threat Reduction Activities* (No. 2020-05), May 2020.
[4] NSIRA, *Review of CSIS Threat Reduction Activities* (No. 2021-04), p. 19. CSIS agreed with this recommendation, emphasizing its commitment to "fully documenting the outcomes of TRMs in a manner consistent with its record-keeping policies."

19. (S) This recommendation was further to SIRC's 2016 Review, which emphasized the importance of documenting TRM outcomes. SIRC commended CSIS for developing guidance with respect to outcome reporting, but urged continued refinement – suggesting, *inter alia*, "timeframes for reporting on all outcomes" – moving forward. CSIS agreed with the recommendation,[5] and successive versions of CSIS's governing policy for TRM have included greater specificity in this regard.[6]

20. (S) A benefit of yearly review is the ability to identify and assess such challenges over time. To this end, each previous NSIRA review, in addition to the particular objectives noted above, tracked and described the overall use of the TRM mandate in the relevant review period. The 2020 review established a dataset of all TRMs since the inception of the mandate in 2015, which in turn helped inform case selection for the 2021 review. Supplemented on an on-going basis by information provided to NSIRA pursuant to subsection 12.1(3.5) of the *CSIS Act*[7], this dataset allows NSIRA to identify trends, patterns, and emerging issues of relevance with respect to CSIS's use of threat reduction measures, including through the quantification of data. Data from a specific year/review period can be contextualized (e.g., was the mandate used more, less, or in a qualitatively different way as compared to previous years?) and topics for future review identified.

21. (S) The present review builds on the above work in two ways. First, we compare the use of the TRM regime in the relevant review period to its use in previous years and identify overall trends and patterns since the inception of the regime. Second, we focus on outcomes by selecting cases of implemented (as opposed to simply proposed or approved) TRMs for review. This speaks not only to the challenges associated with the documentation of outcomes, but also the "rational link" requirement that undergirds a given TRM's reasonableness and proportionality, and globally the alignment of what the measure did with the threat it was intended to reduce. All of these issues have been, to one extent or another, subject to comment, findings, and/or recommendations in previous reviews.

Scope & Objectives

22. (S) The review period covers 1 January 2021 to 31 December 2021. NSIRA also examined information from outside of this period in order to make a full assessment of relevant TRM activities.

23. (U) The review had two main objectives:

---

[5] As a general reply to the review's suite of recommendations, CSIS stated that it was "actively working to ensure threat reduction outcomes are more quantifiable." See SIRC Annual Report 2016-2017, p. 26.
[6] For example, Version 1 of *Conduct of Operations, Section 12.1 Threat Reduction Measures* (effective 20 October 2015) contained no specific timeframe for reporting, while Version 2 (effective 20 November 2017) stated "immediate outcome reports are to be submitted in a timely manner" and Version 3 (effective 21 June 2019) introduced specific junctures at which the Strategic Outcome Report is due. Finally, the current policy (Version 4, effective 23 September 2020) mandates that Implementation Reports (which replaced immediate outcome reports) be filed within five business days of implementation.
[7] According to this provision, CSIS must notify NSIRA "as soon as circumstances permit" following the implementation of a threat reduction measure. NSIRA compiles and tracks these notifications as part of its annual reporting on CSIS activities.

a) Provide an overview of TRMs in 2021, contextualizing the data as appropriate by comparison with data from preceding years and noting any trends or patterns that emerge from the analysis.

b) Conduct a review of a selection of TRMs implemented in 2021.

With respect to this second objective, three TRMs were selected according to criteria designed to maximize the utility of NSIRA's findings and recommendations to CSIS (see the discussion of case selection strategy in Annex C). These TRMs were subject to two lines of inquiry: a compliance review against applicable law, ministerial direction, and policy; and, a review of implementation, including the alignment between what was proposed and what occurred, the documentation of outcomes, and the crucial role of legal risk assessments for guiding CSIS activity.

Sources & Methodology

24. (U) NSIRA examined and considered all relevant legislation and documentation pertaining to the objectives of the review, including:

- (U) The *Canadian Charter of Rights and Freedoms*.
- (U) The *CSIS Act*.
- (U) Ministerial directions issued by the Minister of Public Safety to CSIS.
- (U) CSIS's internal governance framework for TRMs, which included policies, procedures, guidance and training material, tracking systems and cooperation agreements.
- (S) All pertinent TRM documentation, including Requests for Approval (RFAs), Legal Risk Assessments (LRAs), Implementation Reports, Intended Outcome Reports, Strategic Impact Reports, email communications, consultation reports, operational messages, targeting authorities, [redacted] and other relevant documents as available in particular cases.

16(1)(c)(iii)

25. (U) NSIRA employees directly accessed the relevant CSIS databases on 4 March 2022 to collect this information. Subsequent requests (RFIs) for additional documents identified by the review team were issued in March, April and May 2022.

26. (U) The review also analyzed data compiled under previous TRM reviews as well as provided to NSIRA by CSIS pursuant to subsection 12.1(3.5) of the *CSIS Act*.

Confidence Statement

27. (U) NSIRA has high confidence in the information it examined in the course of this review, and consequently in the findings and recommendations emerging therefrom.

28. (U) As noted above, NSIRA employees directly and independently accessed the relevant CSIS database to review and verify information. NSIRA's familiarity[8] with the TRM regime meant that the review team was able to pre-identify relevant TRM documentation and then confirm its existence in CSIS holdings. Following an initial analysis, follow up RFIs targeted specific documents identified as missing or potentially relevant. In some instances, CSIS was able to produce the requested documents; in others, they confirmed that said documents did not exist. This process gave the review team confidence as to the completeness of the documentation necessary to satisfy the objectives of the review. That NSIRA personnel directly retrieved the majority of documents from CSIS databases similarly gives high confidence that the information is valid and accurate. Finally, NSIRA shared a preliminary draft of the report with CSIS to verify its factual accuracy.

[8] This familiarity is the product of past NSIRA and SIRC reviews of section 12.1 measures, as well as the ongoing information provided by CSIS to NSIRA pursuant to subsection 12.1(3.5) of the *CSIS Act*. This baseline of information further boosts NSIRA's confidence with respect to the information sought, obtained, and examined in the course of the present review.

ANALYSIS

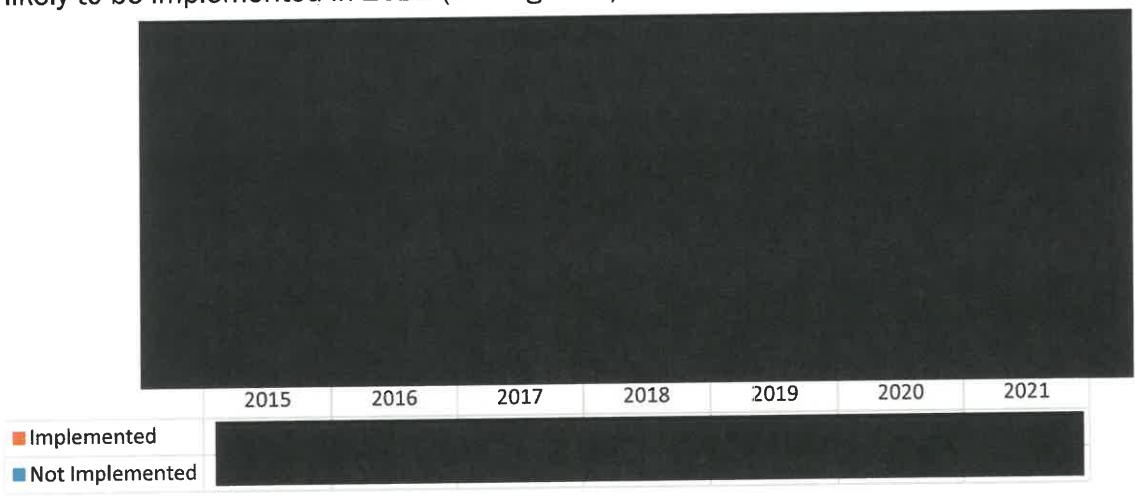
The Review Period in Context

29. (U) The first objective of the review was to document and describe how CSIS used its TRM mandate in 2021, and to contextualize that use by comparison to previous years.

(U) Finding 1: NSIRA finds that CSIS's use of its TRM mandate in 2021 was broadly consistent with its use in preceding years.

30. (S) In 2021, CSIS proposed [redacted] measures (i.e., TRMs designated [redacted]), of which [redacted] were approved and [redacted] implemented. Of the [redacted] TRMs which were approved but not implemented in 2021, all remain valid[9], and implementation rates from previous years suggest that many are likely to be implemented in 2022 (see Figure 1).[10]

15(1)(d)(ii)



15(1)(d)(ii)

(S) Figure 1: Approved TRMs from 2015-2021[11]

31. (S) In addition, [redacted] TRMs that had been proposed in 2020 (designated [redacted]) were ultimately implemented in 2021. Overall, therefore, CSIS implemented [redacted] TRMs a total of [redacted] times during the review period (for an overview, see Table 1 in Annex C).

15(1)(d)(ii)

32. (S) Section 2, paragraphs (a) through (d) of the *CSIS Act* identifies four basic categories of threats to the security of Canada:

16(1)(b)

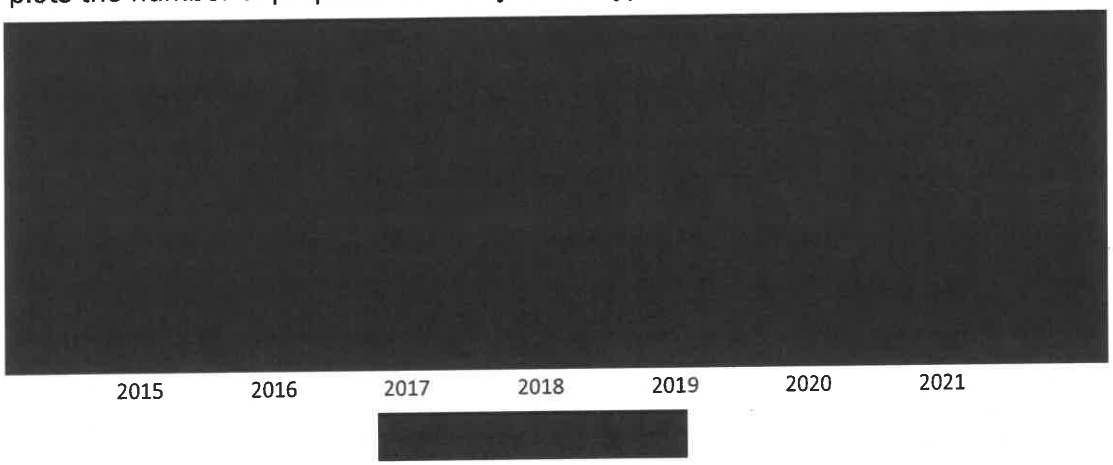
[9] As of April 2022.
[10] CSIS has explained that the level of effort to implement a TRM is substantial (CSIS Briefing by [redacted] TRM to NSIRA on July 9, 2020). Similarly, by the time a TRM is approved its implementation may no longer be an operational priority (e.g., in the context of the threat environment, or because the nature/urgency of a particular threat has shifted). Finally, CSIS may have a menu of approved TRMs against a particular threat, with the implementation of one fulfilling the objectives of the others. Ultimately, implementation rates are useful as a general indicator of how efficiently CSIS is using the mandate, while recognizing that valid operational decisions may keep the rate below 100%.
[11] Each bar represents the ultimate implementation rate for all TRMs approved in a given year, regardless of the year in which implementation first occurred. [redacted]

15(1)(d)(ii)

- Espionage or sabotage (**2a**)
- Foreign interference (**2b**)
- Serious violence for the purpose of achieving a political, religious, or ideological objective (**2c**); and
- Subversion (**2d**).

A range of threats were addressed by measures during the review period, including a rough balance between 2a (espionage/sabotage), 2b (foreign interference), and 2c (violence) threats. [redacted] 2d (subversion) threats, [redacted]

33. (U) This distribution is in keeping with how CSIS used the mandate in previous years. Figure 2 plots the number of proposed TRMs by threat type since 2015.[12]



(S) Figure 2: Proposed TRMs by Threat Type

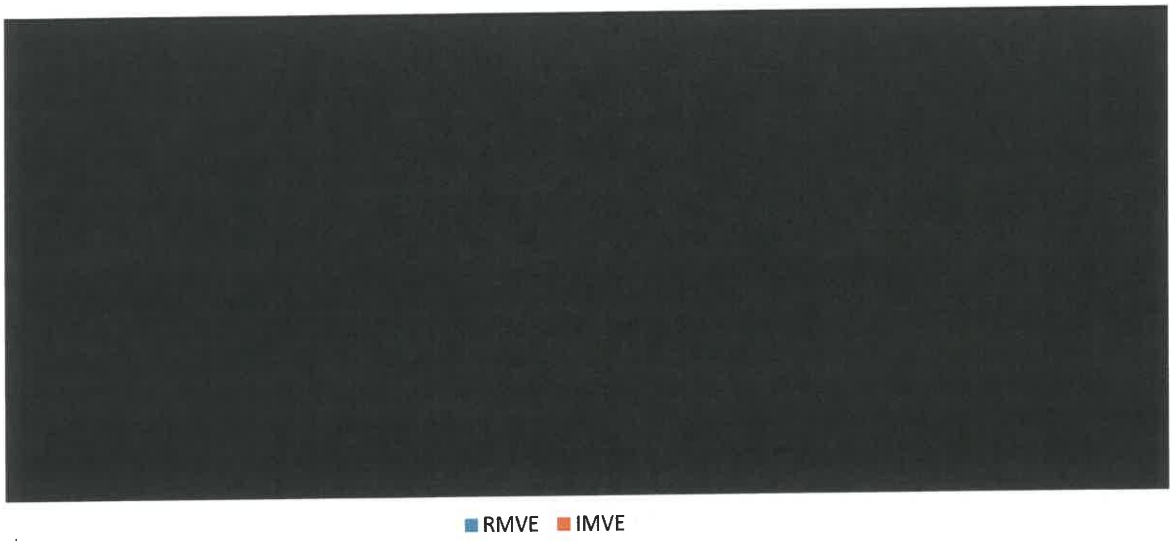
34. (S) Since 2015, 2c (violence) threats have most frequently been the subject of TRMs [redacted] followed closely by 2b (foreign interference) threats.

35. (S) While CSIS's overall focus on 2c threats has been consistent over the years, the underlying composition of those threats (that is, the specific targets within that broader category) has evolved. From 2015-2017, for example, the overwhelming majority of TRMs aimed at reducing 2c threats involved targets associated with religious extremism (what would now be categorized as Religiously Motivated Violent Extremism, or "RMVE"[13]). More recently, and beginning in 2018, there has been an increase in TRMs aimed at targets in the Ideologically Motivated Violent Extremism (IMVE)[14] milieu. Figure 3 shows the number of TRMs in each of these categories year

[12] N.B.: Some TRMs addressed more than one threat type (e.g., 2a *and* 2b) and are therefore double counted in this figure.
[13] From CSIS's *Public Report 2020*, p. 27: "Religiously motivated violent extremism (RMVE) encourages the use of violence as part of a spiritual struggle against a perceived immoral system. Followers believe that salvation can only be achieved through violence."
[14] *Ibid*, p. 26: "Proponents of ideologically motivated violent extremism (IMVE) are driven by a range of influences rather than a singular belief system. IMVE radicalization is more often caused by a combination of ideas and grievances resulting in a...worldview [that] centres on the willingness to incite, enable or mobilize to violence. These individuals and cells often act without a clear affiliation to a specific organized group or external guidance, but are nonetheless shaped by hateful voices and messages online that normalize and advocate violence."

15(1)(d)(ii)

by year.[15]



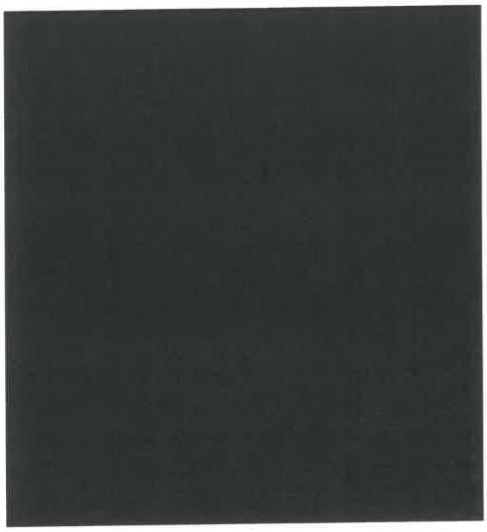
(S) Figure 3: Proposed TRMs within the 2c (violence) threat category, by year

36. (S) Of note, the present review period marks the first time since the inception of the regime that TRMs involving IMVE threats outnumber those stemming from RMVE. [redacted]"[16] This shift in the threat environment is reflected in Figure 3, above, which shows [redacted] with respect to RMVE and IMVE over time.

37. (TS//CEO) There are also trends worth noting with respect to 2b (foreign interference) threats, which have been subject to [redacted] TRMs since 2015. First, the number of TRMs targeting 2b threats [redacted] TRMs in this area aim at reducing threats to Canadian security from hostile state actors; such threats can include, among others, cyber attacks/operations, election interference, or the monitoring of dissidents in Canada. [redacted] throughout the course of the regime, [redacted] (see Figure 4).

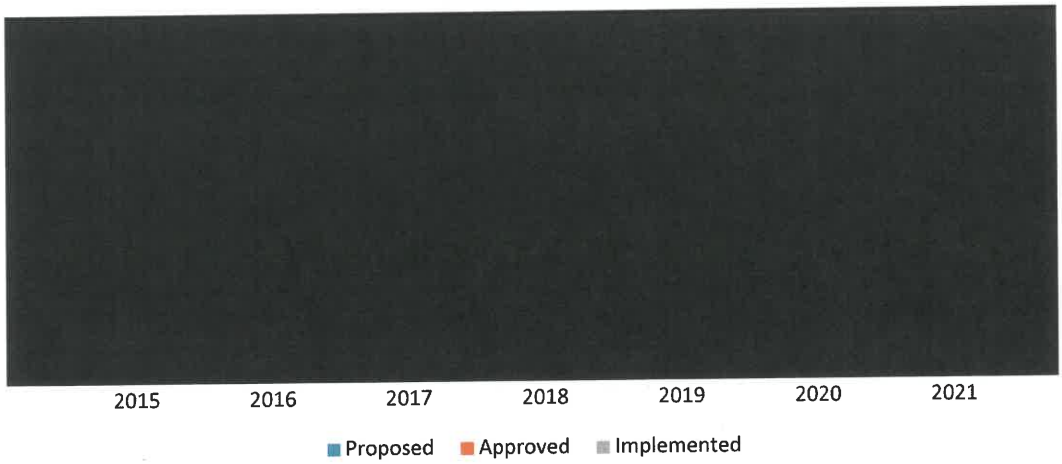
[15] N.B.: In this context, the classification of TRMs as either RMVE or IMVE is an independent and in certain cases retroactive assessment by NSIRA based on available descriptions of the TRMs.
[16] CSIS, 2021-2023 Intelligence Priorities, p. 16.

15(1)(d)(ii)



(TS//CEO) Figure 4: Percentage distribution of TRMs targeting 2b (foreign interference) threats, 2015-2021

38. (S) Figure 5 shows overall trends, specifically use of the regime by TRM status – proposed, approved, and implemented – since 2015. The year 2018 was an inflection point. In that year, CSIS proposed nearly as many TRMs as were proposed in the preceding three years – the first three of the mandate – combined [redacted] In the following year, however, the number dropped slightly [redacted] before a more significant reduction in 2020 [redacted] The year 2020 was a low ebb across all three categories, with the lowest number of implementations [redacted] since the first year of the regime [redacted] This downward trend plateaued during the review period, even rebounding gently. The number of proposed TRMs in 2021 went up as compared to the previous year [redacted] as did both approvals [redacted] and implementations [redacted]



(S) Figure 5: Proposed, Approved, Implemented totals for 2015-2021 TRMs

39. (S) In the course of NSIRA's 2020 TRM Review, CSIS explained [redacted]

[redacted][17] The COVID-19 pandemic interrupted some aspects of that work, such as site visits to regions to explain the program,[18] [redacted] The question of how actively CSIS uses the TRM regime – and whether efforts to bolster its use were or were not successful, or require more attention – is reasonably deferred at present, given the unique circumstances related to COVID-19. Moving forward, however, NSIRA will be attuned to such considerations. Now over five years since the inception of the mandate, an assessment of CSIS's use of TRM as a viable tool complementing the organization's "culture of collection" may warrant explicit consideration.

40. (U) In this way, NSIRA's finding that CSIS's use of TRMs in 2021 is broadly consistent with its use in preceding years is useful as a baseline, or data point, informing future assessments of the regime. Ultimately, each successive year of review will offer additional information and cumulative insight into how CSIS exercises its threat reduction mandate.

Review of Select TRMs

41. (U) NSIRA's second objective was to conduct a review of a selection of TRMs implemented during the review period. NSIRA assessed the TRMs for compliance with applicable law, ministerial direction, and policy. At the same time, NSIRA considered the implementation of each measure, including the alignment between what was proposed and what occurred and, relatedly, the role of legal risk assessments for guiding CSIS activity, as well as the documentation of outcomes. For a full discussion of NSIRA's case selection strategy, see Annex C.

42. (S) The selected cases are as follows[19]:

Case 1

43. (TS) [redacted] CSIS conducted a TRM [redacted][20] [redacted]

44. (S) The TRM involved [redacted][21] [redacted][22]

[17] CSIS Briefing by [redacted] TRM to NSIRA on July 9, 2020. See NSIRA Review 2020-05, "Review of CSIS Threat Reduction Activities," p. 23.
[18] CSIS Briefing by [redacted] TRM to NSIRA on July 9, 2020.
[19] Case 1 is TRM [redacted] Case 2 is TRM [redacted] and Case 3 is TRM [redacted]
[20] "Targeting Authority," [redacted]
[21] [redacted]
[22] As per the RFA this [redacted] "TRM Request for approval (RFA)," Case 1 [redacted]

15(1)(d)(ii)

45. (S//Solicitor-Client Privilege) The Department of Justice (hereafter, "Justice") provided CSIS with a Legal Risk Assessment (LRA) of the proposed TRM [23]

15(1)(d)
23

46. (S)

15(1)(d)(i)

47. (S) Following these implementations, CSIS assessed that the immediate intended outcomes of the TRM "[27]

15(1)(d)(i)

"[28]

48. (S) The TRM's Strategic Impact Report, ultimately concluded that the TRM's

15(1)(d)(ii)

[29]

Case 2

49. (TS) CSIS conducted a TRM

15(1)(d)(ii)

[30] [31]

50. (S) The TRM

15(1)(d)(ii)

16(1)(b)

---

[23] 23

[25]

[26]

[27] "Intended Outcome Report," Case 1 15(1)(d)(ii)

[28]

[29] "Strategic Impact Report," Case 1

[30] "TRM Request for approval (RFA)," Case 2

[31] "Targeting Authority," Case 2

15(1)(d)(ii)
16(1)(b)

[redacted]"[32]

51. (S//Solicitor-Client Privilege) Justice delivered an LRA of the proposed TRM to CSIS [redacted]

23

[redacted][33]

[redacted]"[34]

15(1)(d)(ii)

52. (S) CSIS implemented the TRM [redacted]

53. (TS) Following the first implementation, CSIS assessed that the immediate intended outcome of the TRM had been "met". [redacted]

15(1)(d)(i)
16(1)(b)

[redacted].[35]

[redacted]"[36]

[redacted][37]

[redacted]"[38]

54. (TS) [redacted] the TRM's Strategic Impact Report, [redacted]

15(1)(d)(ii)
16(1)(b)

[redacted][39]

[redacted]"[40]

Case 3

55. (TS//CEO) [redacted] CSIS conducted a TRM [redacted]

15(1)(d)(ii)

[redacted]

---

[32] "TRM Request for approval (RFA)," Case 2 [redacted] 15(1)(d)(ii)
[33] [redacted] 23
[34] *Ibid.* [redacted]
[35] "Implementation and Intended Outcome Report," Case 2 [redacted]
[36] "Implementation and Intended Outcome Report II," Case 2 [redacted] 15(1)(d)(ii)
[37] [redacted]
[38] [redacted]
[39] "Strategic Impact Report," Case 2 [redacted]
[40] [redacted]

[41] 15(1)(d)(ii)

56. (S//CEO) The TRM involved [42].

15(1)(d)(ii)
16(1)(b)

57. (S//Solicitor-Client Privilege) Justice did not provide a formal LRA in this case. [43]

15(1)(d)(ii)
16(1)(b)
23

"[44]

58. (S) CSIS implemented the TRM [45]

15(1)(d)(ii)
16(1)(b)

[46]

59. (S) CSIS assessed that [47]

15(1)(d)(ii)
16(1)(b)

[48]

[49]

Compliance with the law

[41] "Targeting Authority," Case 3
[42] CSIS itself *Ministerial Direction for Accountability*, 2019,
[43] See the discussion of "TRM Modernization" in text box on page 21.
[44]
[45] This group "Implementation Report," Case 3 15(1)(d)(ii)
[46] "Implementation Report," Case 3
[47] "Intended Outcome Report," Case 3
[48]
[49]

(U) Finding 2: For all the cases reviewed, NSIRA finds that CSIS met its obligations under the law, specifically the *Canadian Charter of Rights and Freedoms* and sections 12.1 and 12.2 of the *CSIS Act*.

60. (U) As made explicit by subsection 12.1 (3.1) of the *CSIS Act*, the *Charter* "is part of the supreme law of Canada and all [TRMs] shall comply with it." Measures that would limit a right or freedom protected by the *Charter* may only be undertaken if authorized by a warrant.[50] However, the TRMs under consideration in this review were non-warranted measures. NSIRA's assessment of *Charter* compliance considered whether any protected right or freedom was limited as a result of the measure. Examination of outcome reporting and other relevant documentation indicated that no such limitations occurred.[51]

61. (U) The key requirements of sections 12.1 and 12.2 of the *CSIS Act* include:

- *Reasonable grounds to believe*. In order to conduct a threat reduction measure, CSIS must demonstrate that it has a "reasonable grounds to believe" (RGB) that a particular activity constitutes a threat to the security of Canada. The information and intelligence provided to support this threshold must be credible, compelling, and reliable.
- *Reasonableness and Proportionality*. The measures must be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat and the reasonably foreseeable effects on third parties, including on their right to privacy.
- *Consultation*. Before conducting a threat reduction measure, CSIS must consult, as appropriate, with other federal departments as to whether they are in a position to reduce the threat.
- *Warrant requirements*. Any threat reduction measure that would limit a right or freedom guaranteed by the *Charter*, or would otherwise be contrary to Canadian law, can only be conducted if authorized by a warrant issued by a judge pursuant to section 21.1 of the *CSIS Act*.
- *Prohibited conduct*. No threat reduction measure may involve conduct prohibited by subsection 12.2(1) of the *CSIS Act*.[52]

62. (S//Solicitor-Client Privilege) For the measures reviewed, each RFA explicitly addressed the requirements for RGB, reasonableness and proportionality, and consultations with other federal

[50] Of note, CSIS has not yet sought judicial authorization for a TRM under subsection 12.1 (3.2). Accordingly, the relevant provisions of the *CSIS Act* have never been subject to interpretation by the courts.

[51] This finding considered only the outcome of the TRMs. As discussed below (at paragraph 83), the question of whether [redacted] 15(1)(d)(ii) 23

[52] Specifically, CSIS shall not: (a) cause, intentionally or by criminal negligence, death or bodily harm to an individual; (b) willfully attempt in any manner to obstruct, pervert or defeat the course of justice; (c) violate the sexual integrity of an individual; (d) subject an individual to torture or cruel, inhuman or degrading treatment or punishment, within the meaning of the Convention Against Torture; (e) detain an individual; or (f) cause the loss of, or any serious damage to, any property if doing so would endanger the safety of an individual.

15(1)(d)(ii)
23

departments. In addition, the two LRAs (for Case 1 and Case 2, respectively) and one legal consultation (for Case 3) addressed [redacted] Similarly, the LRAs for Case 1 and Case 2 determined that the proposed TRMs [redacted]

63. (U) NSIRA broadly concurred with these assessments and conclusions. Further, but for Case 3 (see paragraph 79, below), there was no information in the relevant implementation reports or associated documentation that indicated that the actual implementation of the measures sufficiently deviated from the proposed implementation as to be of concern. Finally, NSIRA determined that none of the implemented measures involved any conduct prohibited by subsection 12.2(1) of the *CSIS Act*.

64. (U) In addition to general legal compliance, NSIRA paid particular attention to the "rational link" test that helps CSIS establish the reasonableness and proportionality of a measure. As noted above, NSIRA's 2020 TRM review cautioned against overly broad rational link criteria while also finding that the rational link had not been met in the selection of certain individuals for inclusion in a TRM. As such, the present review assessed whether a) the proposed rational link was logical and clear; and b) that it was met for each proposed implementation.

(U) Finding 3: For all the cases reviewed, NSIRA finds that CSIS sufficiently established a "rational link" between the proposed measure and the identified threat.

65. (U) However, NSIRA notes several legal and operational considerations that were not addressed as part of the design and analysis of the proposed TRMs but which may be relevant to the contemplation and evaluation of future, similar, measures.

66. (S//Solicitor-Client Privilege) For Case 1, [redacted]

15(1)(d)
16(1)(b)
23

67. (S) While none of these [redacted] undermine NSIRA's finding of legal compliance, they do underscore the possible challenges and risks associated with TRMs involving [redacted]

15(1)(d)(ii)
16(1)(b)

68. (S//Solicitor-Client Privilege) For Case 2, [redacted]

15(1)(d)(ii)
23

[53] [redacted] Case 1 [redacted] 23

[54] [redacted] 15(1)(d)(ii)

[redacted][55] In the certification for the second implementation of the TRM, in which an assessment of, and statement regarding, reasonableness and proportionality is required, [redacted] 15(1)(d)(ii)
[redacted][56] Again, while it is unlikely that such [redacted] had they been considered, would have 23
rendered the second implementation unreasonable and/or disproportional in this case, the lack of consideration is potentially informative for other TRMs [redacted] and, even if minimal, may need to be addressed in certifications of the reasonableness and proportionality of each [redacted] implementation.

69. (TS//Solicitor-Client Privilege) Finally, for Case 3, [redacted] 15(1)(d)(ii)
23
NSIRA's 2021 TRM review dealt extensively with the question of CSIS's relationship with third parties. Case 3 underscores several of NSIRA's findings and recommendations from that review, in particular regarding the need to consider plausible adverse impacts of TRMs involving third parties and to document third party activity following implementation.

Compliance with ministerial direction

(U) Finding 4: For Case 1 and Case 2, NSIRA finds that CSIS met its obligations under the 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* issued by the Minister of Public Safety.

(U) Finding 5: For Case 3, NSIRA finds that CSIS did not meet its obligations under the 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* issued by the Minister of Public Safety.

70. (S) Case 3 involved: [redacted] 15(1)(d)(ii)

71. (S) A "fundamental principle" of the 2015 MD is that "the greater the risk associated with a particular activity, the higher the authority required for approval."[57] This principle was reflected in the section 12 targeting authority [redacted] which states [redacted] approval was required [redacted][58] [redacted] 15(1)(d)(ii)

---

[55] [redacted] Case 2 [redacted] 23
15(1)(d)(ii) [56] [redacted] Case 2 [redacted]
[57] An associated General Direction further states that, with respect to CSIS's collection, threat reduction, analysis, and advisory activities: "The level of authority required for approving the use of intrusive operational techniques must be commensurate with their intrusiveness and with any risks associated with using them. In addition, more senior levels of approval must be obtained for: investigations that affect [redacted] 15(1)(d)(ii)
[58] "Targeting Authority," Case 3 [redacted] Elsewhere the document states, [redacted]

[redacted] ultimately means the *letter* of the fundamental principle regarding the calibration of level of risk and level of approval was met, NSIRA finds that the *spirit* of the principle was not honoured in this case.[59] NSIRA believes that [redacted]

15(1)(d)

72. (S) In response to a preliminary draft of the present report, CSIS noted to NSIRA that the presence of the [redacted] see footnote 45 above – in the implementation of the TRM reflected CSIS's recognition as to the sensitivities of this case. CSIS further argued that risks associated with [redacted] NSIRA agrees that *part* [redacted] In addition, however, [redacted] These risks are not, and in the instance of Case 3 were not, captured by CSIS's reputational risk assessment. [redacted]

15(1)(d)(ii)

73. (S//Solicitor-Client Privilege) The 2019 MD addresses this risk assessment process. Annex A of the MD requires CSIS operational activities, including TRMs, to undergo a four-pillar assessment for legal, operational, reputational, and foreign policy risk. According to the MD, "Legal risk is to be assessed in accordance with the Department of Justice risk assessment criteria." As noted in paragraph 57, above, no formal Legal Risk Assessment (LRA) was produced for Case 3. [redacted] (See the below textbox for a discussion of TRM Modernization [redacted]

23

CSIS's TRM Modernization Project

CSIS implemented the TRM Modernization Project on 19 January 2021, [redacted] The new process reduces the [redacted] aligns TRMs with other programs [redacted][60]

15(1)

As per the new process outlined in the *Department of Justice (DOJ) Legal Risk Management Framework* (which supports Justice/CSIS engagement on TRM), Justice advice via an LRA would be sought only where [redacted] would be encountered by the TRM. (Prior to this, formal LRAs had been provided as part of every

[59] Recall that a section 12 targeting authority requires an RGS standard, whereas a section 12.1 TRM requires the RGB standard. If the calibration of level of risk with level of approval applies to activities with a lower evidentiary standard (RGS), it is reasonable to conclude that a similar calibration ought to obtain for activities subject to a higher standard (RGB).
[60] "TRM Modernization Project", Powerpoint presentation, n.d.

TRM proposal.)

15(1)
16(1)(b)

[redacted]61

74. (S//Solicitor-Client Privilege) Setting aside whether or not the TRM did or did not meet any of [redacted] (we return to this consideration below), NSIRA does not believe the legal advice fulfilled the requirements for legal risk assessments set out in the 2019 MD. [redacted]

15(1)(d)(ii)
23

However, CSIS's Overall Risk Assessment (ORA), which evaluates all four pillars of risk identified by the 2019 MD, [redacted] an absence [redacted] for an LRA was taken by CSIS to imply [redacted] which contributed to the ORA's overall calculation that the TRM was low risk.[62] Again, determining the legal risk level in this way [redacted] rather than a consideration of the actual legal risks themselves) does not comply with the ministerial direction that legal risk be assessed "in accordance with the Department of Justice risk criteria."

75. (S//Solicitor-Client Privilege) The pre-identification of [redacted] if met, would require formal LRAs, is part of CSIS's TRM Modernization project, launched in January 2021 (see textbox on TRM Modernization, above). An assessment of this new legal risk assessment model is beyond the scope of the present review, though may warrant attention in future years. In the present context, however, NSIRA questions the conclusion that Case 3 did not meet any of the identified [redacted] for consultation. Specifically, NSIRA believes the TRM may have met [redacted] and did meet [redacted]

15(1)(d)(ii)
23

61 [redacted]
62 [redacted]

76. (S//CEO//Solicitor-Client Privilege) [redacted] a formal consultation (LRA) must be produced for TRMs "where [redacted][63] [redacted][64] [redacted] NSIRA believes that the cumulative effects [redacted] ought to have been explicitly considered as part of the TRM. This would have allowed CSIS to determine whether such risks were sufficient [redacted]

15(1)(d)(ii)
16(1)(b)
23

77. (S) To be clear, it is not NSIRA's position that the cumulative effects *were* unreasonable in this case, or constituted an abuse of process; rather, the *risks* that they were, or did, ought to have been considered more explicitly, which could then have [redacted] a formal LRA, as per the process established by TRM Modernization.

15(1)(d)(ii)

78. (S//Solicitor-Client Privilege) [redacted]"[65] [redacted].[66] [redacted]

15(1)(d)(ii)
23

79. (S//Solicitor-Client Privilege) In addition to [redacted] under the current governance regime, NSIRA notes that the absence of a comprehensive legal assessment had potential consequences during the implementation of Case 3.

15(1)(d)(ii)
23

80. (S//Solicitor-Client Privilege) NSIRA observed that there was a discrepancy in terms of how CSIS described the measure in its proposal [redacted]"[67], [redacted]

15(1)(d)(ii)
23

---

[63] "[redacted]" document provided to NSIRA from CSIS pursuant to [redacted]

[64] "TRM Request for Approval (RFA)," Case 3 [redacted]

[65] [redacted] document provided to NSIRA from CSIS pursuant to [redacted]

15(1)(d)(ii)
23

[66] These were [redacted] – was also identified as possessing similar characteristics, [redacted]

[67] "TRM Request for Approval (RFA)," Case 3 [redacted]

15(1)(d)(ii)
23

[redacted].[68] [redacted]

81. (S//Solicitor-Client Privilege) The RCMP raised the question of timing during consultations with CSIS about the TRM: [redacted]

13(1)
15(1)(d)(ii)
23

[redacted]"[69] [redacted]

82. (S//Solicitor-Client Privilege) [redacted]

15(1)(d)(ii)
23

[redacted] More generally, NSIRA highlights the risks created by ambiguity in the implementation of a TRM, particularly absent clear consideration of possible risks as would occur in an LRA.

83. (S//Solicitor-Client Privilege) [redacted]

15(1)(d)(ii)
23

[redacted]

[68] [redacted] 15(1)(d)(ii)
[69] "Consultation with RCMP: Record of Decision," Case 3 [redacted]

84. (S//Solicitor-Client Privilege) These considerations are illustrative. The fundamental point is that [redacted]

(U) Recommendation 1: NSIRA recommends that formal Legal Risk Assessments (LRAs) be conducted for TRMs [redacted]

85. (S) This recommendation reflects the explicit emphasis placed on these categories by the 2015 MD as well as elsewhere in CSIS policy. While NSIRA understands the desire to streamline the TRM process – reflected in the changes made to legal risk assessment under TRM Modernization – the risks associated with TRMs [redacted] rather than situational. A standing policy – [redacted] – is therefore appropriate in these cases.

86. (U) It was beyond the scope of the present review to consider the TRM Modernization model in its entirety. The above findings and associated recommendation, however, highlight potential discordance between the application of that model and the requirements of ministerial direction, particularly with respect to legal risk assessments in certain cases.

(U) Recommendation 2: NSIRA recommends that CSIS consider and evaluate whether legal risk assessments under TRM Modernization comply with applicable ministerial direction.

87. (U) Such an evaluation would allow CSIS to close potential compliance gaps and ensure that legal risk assessments – a mandatory component of every TRM – fulfill their intended function.

Legal Risk Assessments (LRAs)

88. (S//Solicitor-Client Privilege) [redacted] These assessments ultimately bear on implementation – should CSIS deviate too widely from what they said they would do, the legal risk assessment they received may no longer fully apply, or additional risks may be created that were not considered.

(U) Finding 6: With respect to Legal Risk Assessments (LRAs), NSIRA finds that greater specificity regarding legal risks, and direction as to how risks could be mitigated and/or avoided, resulted in more detailed outcome reporting vis-à-vis legal compliance.

89. (S) This finding emerges from a comparative analysis of the [redacted] for Case 3; see Recommendation #1).

90. (S) The fact patterns for Case 1 and Case 2 were very similar. Each TRM involved [redacted] Nonetheless, NSIRA observed slight but relevant differences between the LRAs offered [redacted]

91. (S//Solicitor-Client Privilege) [redacted][70] [redacted][71] [redacted][72] [redacted]

92. (S//Solicitor-Client Privilege) [redacted][73] [redacted]"[74] This reflects an understanding of the limits [redacted] and the care taken by investigators to stay within them.

93. (S//Solicitor-Client Privilege) [redacted]

94. (S//Solicitor-Client Privilege) [redacted]

---

[70] "[redacted]
[71] [redacted]
[72] In previous TRM reviews, when examining TRMs involving [redacted]
[73] "Implementation and Intended Outcome Report," Case 2 [redacted] and "Implementation and Intended Outcome Report II," Case 2 [redacted]
[74] "Implementation and Intended Outcome Report," Case 2 [redacted]
[75] [redacted]

[redacted][76] For example, in the Implementation Report for [redacted]"[77] [redacted]

(U) Recommendation 3: NSIRA recommends that CSIS work with the Department of Justice to ensure that Legal Risk Assessments (LRAs) include clear and specific direction regarding possible legal risks and how they can be avoided/mitigated during implementation of the TRM.[78]

95. (S) A comparative assessment of [redacted] suggests to NSIRA that clarity and specificity regarding legal risks and how they can be mitigated/avoided serves to guide investigators during the implementation phase.[79] The associated recommendation would allow investigators, whether new or experienced, to be aware of, and understand, the parameters within which they can operate without breaching the *Charter* or the law, as well as the delimitations of the line(s) that, if crossed, would constitute a breach (or create a significant risk thereof) according to Justice.

96. (U) This may also improve both implementation and associated reporting. Providing clear guidelines would prompt CSIS investigators to specify in their implementation reports how they remained within the delimitations.

(U) Recommendation 4: NSIRA recommends that Implementation Reports specify how the legal risks identified in the LRA were avoided/mitigated during implementation of the TRM.

[76] "Implementation Report [redacted] Case 1 [redacted] "Implementation Report [redacted]" Case 1 [redacted] and "Implementation Report [redacted] Case 1 [redacted]

[77] "Implementation Report [redacted] Case 1 [redacted]

[78] This echoes the recommendation offered in NSIRA's "Review arising from Federal Court's Judgment in 2020 [redacted] – in which CSIS and Justice work collaboratively and iteratively to achieve operational goals within the bounds of the law – as a best practice.

[79] NSIRA recognizes that the [redacted] Nonetheless, the comparison [redacted] is useful for generating insight that may be relevant in the formulation of such assessments moving forward.

97. (U) The significant powers bestowed by the TRM mandate create potential risks to the rights and freedoms of the individuals subject to such measures, or others captured by their scope. Including specific reporting about how identified risks were mitigated or avoided in the implementation of a TRM would allow CSIS to demonstrate that it was legally compliant from start (what they proposed to do) to finish (what they did) in each case, thereby bolstering confidence that the regime is being used responsibly.[80] (See also the discussion of TRM documentation beginning at paragraph 101, below.)

Compliance with policy

98. (S) TRM governance includes requirements that specifically address relevant statutory obligations. For example, [redacted] 15(1) In this way, compliance with policy is crucial for ensuring compliance with the law.

(U) Finding 7: For Case 2 and Case 3, NSIRA finds that CSIS did not meet its obligations with respect to one requirement of its *Conduct of Operations, Section 12.1 Threat Reduction Measures*, Version 4. CSIS did not meet its internal policy requirements regarding the timelines to submit TRM implementation reports.

99. (S) Specifically, NSIRA found that:

- For Case 2, the report for the second implementation of the measure was not submitted within five business days (as per paragraphs 6.2 and 6.3 of the *Conduct of Operations*, Version 4). [redacted][81]
- For Case 3, the report for the implementation of the measure was not submitted within five business days (as per paragraph 6.2 of *Conduct of Operations*, Version 4). [redacted][82] 15(1)(d)(ii)

100. (S) This non-compliance is minor in nature. However, it should be noted that delay in drafting and submitting implementation reports could conceivably impact their depth, rigour, and accuracy, particularly as the reports involve a detailed description of what occurred during implementation. If submitting implementation reports within five business days is chronically challenging for investigators, CSIS may wish to revisit the policy requirement and adjust it accordingly.[83]

---

[80] In response to a preliminary draft of the present report, CSIS stated that implementing Recommendation 4 would create an "administrative burden…with no clear benefit." NSIRA nonetheless emphasizes the benefits – documentation of legal compliance – of this approach. Further, clear legal guidance in LRAs (see Recommendation 3, above) would facilitate the recommended practice.

[81] "Implementation and Intended Outcome Report II," Case 2 [redacted] 15(1)(d)(ii)

[82] "Implementation Report," Case 3 [redacted]

[83] In response to a preliminary draft of the present report, CSIS explained that a revision from a 5-day to a 10-day requirement is forthcoming, in recognition that the current timeframe is challenging given resourcing constraints.

Documentation of outcomes

101. (S) More generally, the documentation of implementation and outcomes is important, for at least two reasons. First, to ensure that *ex ante* compliance obtains *ex post*. The key consideration here is the alignment between what CSIS proposed to do and what they ultimately did. Second, so that CSIS can evaluate what worked and what did not, with an eye toward future TRMs. Were the goals articulated in the RFA achieved? Did the measure reduce the threat? Knowing the answers to these questions is crucial for determining both what to do next (with respect to a particular threat actor) and what to do in the future (vis-à-vis other, broadly comparable threat actors or circumstances).

(U) Finding 8: For Case 3, NSIRA finds that the Intended Outcome Report was not completed in a timely manner.

102. (S) At the time NSIRA initially collected information for this review [redacted] it did not find an Intended Outcome Report for Case 3 in the relevant CSIS database. In a follow-up request for information, dated [redacted] NSIRA sought to confirm whether or not an Intended Outcome report for this TRM had been produced. CSIS provided the report to NSIRA on [redacted] the completion date for the report was a day earlier, [redacted]

103. CSIS explained that the relevant regional desk was waiting to receive information from an external party, and therefore was not in a position to complete the Intended Outcome Report at an earlier date.[84] Nonetheless, NSIRA notes that the Intended Outcome Report dated [redacted] provided relevant and valuable information, even as the information from the external party remained outstanding.

104. (S) CSIS's policy on when Intended Outcome (what CSIS formerly called "intermediate outcome") Reports are required is unclear. Paragraph 6.5 of CSIS's *Conduct of Operations, Section 12.1 Threat Reduction Measures,* Version 4 discusses the need for both Intended Outcome and Strategic Impact reports but only specifies when the latter is due (more on this below, see paragraph 109). As such, the above finding is not a compliance issue, but instead relates to the effective use of such reports for informing CSIS operations. Particularly insofar as CSIS contemplates additional TRMs – or additional implementations of the same TRM under a standing authority – against the same threat actor, having intended outcome reports in hand would likely be of use to operational units and approval authorities.

105. (S) This was specifically true with respect to [redacted] for example. [redacted]"[85] [redacted]"[86] [redacted]

[84] CSIS response to NSIRA, 2 September 2022.
[85] "Targeting Authority," Case 3 [redacted]
[86] *Ibid.* [redacted], emphasis added]

[redacted] Particularly when such key decision points arise, information as to the outcome of a TRM is relevant and potentially useful.

106. (S) As noted in the case description at paragraph 59 above, CSIS ultimately determined that, as of January 2022, [redacted]"[87] [redacted] That the Intended Outcome report was not completed until [redacted] suggests that this information was not available (or at least not documented) in a timely manner.

(U) Recommendation 5: NSIRA recommends that CSIS specify in its *Conduct of Operations, Section 12.1 Threat Reduction Measures* when the Intended Outcome Report is required, as it does for the Strategic Impact Report.

107. (S) This recommendation would mean that [redacted] reporting requirements would be subject to explicit timeframes, adding to those currently in place for Implementation Reports (within five business days) and Strategic Impact Reports (at one of two specified junctures). Determining when the Intended Outcome Report ought to be completed will require careful consideration. NSIRA's recommendation does not include a specific timeframe, only that CSIS take the steps to determine what is practical and, in light of the considerations above, useful in this regard (e.g., provides relevant information in a timely manner, particularly with respect to key decision points such as renewals of authorities). While NSIRA acknowledges CSIS's position that outstanding information may present challenges to an explicit timeframe, we also highlight the pertinent information that was ultimately included in the [redacted] Intended Outcome Report for Case 3. This example demonstrates the potential value of reporting information in hand as opposed to waiting until all information is received, with the recognition that updates can always be appended as new information becomes available.

108. (S) The spirit of the recommendation is that more information, sooner, is beneficial for CSIS as it conducts TRMs. As the above analysis of Case 3 makes clear, knowing outcomes is important not only for tracking the success or failure of the TRM itself, but also for understanding how the TRM factors into the ongoing section 12 investigation within which it occurred. This includes the development of possible subsequent TRMs against the same threat actor. [redacted][88] [redacted]"[89] [redacted][90] [redacted]

[87] "Intended Outcome Report," Case 3 [redacted]
[88] [redacted]
[89] [redacted]
[90] See for example [redacted] way forward," email correspondence, [redacted] Case 2 [redacted]

109. (S) Current CSIS policy allows the Strategic Impact report to be completed at *either*:

- the expiry of the TRM authority, *or*
- the closing of the investigative authority related to the TRM.

In practice, because a TRM authority [redacted]

(U) Finding 9: NSIRA finds that current policy for the completion of Strategic Impact Reports may inhibit the timely production of important information.

110. (S) Of note, the above analysis with respect to the Intended Outcome Report for Case 3 is equally applicable to its Strategic Impact Report. The TRM authority for Case 3 [redacted]

111. (S) For Case 1, CSIS completed the Strategic Impact Report [redacted] just before the expiry of the TRM authority [redacted]

(U) Recommendation 6: NSIRA recommends that CSIS integrate in policy a requirement that the Strategic Impact Report be completed at the expiry of the TRM authority.

112. (S) This recommendation urges CSIS to produce relevant information sooner, rather than later. Given that strategic outcomes may influence or inform decision-making on further TRMs *within* active investigations, assessing outcomes *prior* to the closing of those investigations makes sense. If the strategic impact remains unclear at this earlier juncture (as may be the case for TRMs with short validity periods, e.g., 90 days) the relevant report can say as much and the issue can be revisited as necessary at the closing of the investigative authority. NSIRA notes that in the three cases under review, CSIS completed the Strategic Impact Report at the earlier of the two junctures

(closing of the TRM authority); the above recommendation would simply codify this practice[91].

[91] In response to a preliminary draft of the present report, CSIS explained that a new "TRM Outcome Report" is set to replace both the Intended Outcome Report and the Strategic Outcome Report, and will be due at the expiry of the TRM authority. At the time of writing, however, the revision is not yet in place.

CONCLUSION

113. (U) Overall, NSIRA found that CSIS's use of its TRM mandate in 2021 was broadly consistent with its use in preceding years. With respect to the TRMs reviewed, NSIRA found that CSIS met its obligations under the law, specifically the *Canadian Charter of Rights and Freedoms* and sections 12.1 and 12.2 of the *CSIS Act*. For one of the measures, however, NSIRA found that CSIS did not meet its obligations under the 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* issued by the Minister of Public Safety.

114. (S) The review contextualized CSIS's use of TRMs in 2021 against its historical use of the regime. Of note, the decrease that began after 2018 plateaued in 2021 – NSIRA even observed modest upticks in TRM proposals, approvals, and implementations in the present review period. Moving forward, and out of the COVID-19 pandemic, monitoring and analyzing these numbers will inform future review.

115. (U) The targeted objective of this year's review was to conduct a review of a selection of implemented TRMs. In so doing, NSIRA was mindful of observations, findings, and recommendations emerging from previous SIRC and NSIRA reviews, for example the requirement that the "rational link" (between selected subject and threat) be present in each case, and that the documentation of outcomes be clear and complete. The focus on implementation generally raised the question of alignment between what CSIS proposed to do and what ultimately occurred.

116. (U) Within this line of inquiry, findings and recommendations emerged which underscore NSIRA's belief that relevant information, available in a timely manner, benefits CSIS operations. While cognizant that overly burdensome documentation requirements can unduly inhibit CSIS activities, NSIRA nonetheless believes that the recommendations provided here are prudent and reasonable, less creating new requirements as much as sharpening and refining existing ones.

117. (S) [redacted] This analysis touched both directly and indirectly on the new – as of January 2021 – legal risk assessment model in place pursuant to CSIS's "TRM Modernization". 15(1)(d)(ii) 23 While the review did not consider this model *in toto*, and could not therefore pass comment on its performance, [redacted] NSIRA recommended closing the gap by requiring an LRA for any TRMs [redacted] and further recommended that CSIS evaluate the new model against the requirements of ministerial direction, particularly those associated with legal risk assessments. Moving forward, a focused NSIRA review of TRM Modernization may take up these questions with an eye toward compliance more broadly, as well as possible additional recommendations addressing gaps, issues, or risks.

118. (S) Relatedly, the present review emphasized the importance of the guidance and direction offered in LRAs, both for identifying and mitigating potential legal risks and, crucially, for ensuring that CSIS investigators stay within the bounds of legal compliance during actual implementation of the TRM. Clear advice allays ambiguity and uncertainty, minimizing the potential for inadvertent

breaches as CSIS employees implement the measure, while making it easier for employees to document legal compliance in after-action reporting.

119. (U) The result is enhanced likelihood that CSIS will use the TRM mandate lawfully and responsibly. In this vein, it bears underscoring the general finding of compliance – with law, ministerial direction, and policy – at the core of this review, noted issues notwithstanding.

ANNEX A: FINDINGS & RECOMMENDATIONS

Findings

(U) **Finding 1:** NSIRA finds that CSIS's use of its TRM mandate in 2021 was broadly consistent with its use in preceding years.

(U) **Finding 2:** For all the cases reviewed, NSIRA finds that CSIS met its obligations under the law, specifically the *Canadian Charter of Rights and Freedoms* and sections 12.1 and 12.2 of the *CSIS Act*.

(U) **Finding 3:** For all the cases reviewed, NSIRA finds that CSIS sufficiently established a "rational link" between the proposed measure and the identified threat.

(U) **Finding 4:** For Case 1 and Case 2, NSIRA finds that CSIS met its obligations under the 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* issued by the Minister of Public Safety.

(U) **Finding 5:** For Case 3, NSIRA finds that CSIS did not meet its obligations under the 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* issued by the Minister of Public Safety.

(U) **Finding 6:** With respect to Legal Risk Assessments (LRAs), NSIRA finds that greater specificity regarding legal risks, and direction as to how said risks could be mitigated and/or avoided, resulted in more detailed outcome reporting vis-à-vis legal compliance

.

(U) **Finding 7:** For Case 2 and Case 3, NSIRA finds that CSIS did not meet its obligations with respect to one requirement of its *Conduct of Operations, Section 12.1 Threat Reduction Measures*, Version 4. CSIS did not meet its internal policy requirements regarding the timelines to submit TRM implementation reports.

(U) **Finding 8:** For Case 3, NSIRA finds that the Intended Outcome Report was not completed in a timely manner.

(U) **Finding 9:** NSIRA finds that current policy for the completion of Strategic Impact Reports may inhibit the timely production of important information.

Recommendations

15(1)(d)(ii)

(U) **Recommendation 1:** NSIRA recommends that formal Legal Risk Assessments (LRAs) be conducted for TRMs [redacted]

(U) **Recommendation 2:** NSIRA recommends that CSIS consider and evaluate whether legal risk assessments under TRM Modernization comply with applicable ministerial direction.

(U) **Recommendation 3:** NSIRA recommends that CSIS work with the Department of Justice to ensure that Legal Risk Assessments (LRAs) include clear and specific direction regarding possible legal risks and how they can be avoided/mitigated during implementation of the TRM.

(U) **Recommendation 4:** NSIRA recommends that Implementation Reports specify how the legal risks identified in the LRA were avoided/mitigated during implementation of the TRM.

(U) **Recommendation 5:** NSIRA recommends that CSIS specify in its *Conduct of Operations, Section 12.1 Threat Reduction Measures* when the Intended Outcome Report is required, as it does for the Strategic Impact Report.

(U) **Recommendation 6:** NSIRA recommends that CSIS integrate in policy a requirement that the Strategic Impact Report be completed at the expiry of the TRM authority.

ANNEX B: TRM MANDATE

(U) In June 2015, Parliament enacted the *Anti-terrorism Act, 2015*, which authorized CSIS, in the new section 12.1 of the *CSIS Act*, to take measures to reduce threats to the security of Canada, within or outside Canada.[92] The new measures represented an unprecedented departure from CSIS's traditional intelligence collection role.

(U) In July 2019, the *National Security Act, 2017*, introduced amendments to CSIS's TRM mandate that sought to clarify and further define this power. In particular, the amendments stressed the importance of compliance with the *Canadian Charter of Rights and Freedoms* (*Charter*), provided an expanded list of prohibited conduct under the TRM regime,[93] and introduced a requirement that CSIS notify NSIRA after undertaking a TRM.

(U) The *CSIS Act* does not provide a precise definition of "measures to reduce the threat." As such, CSIS has developed its own, defining a TRM as "[a]n operational measure undertaken by [CSIS], pursuant to section 12.1 of the *CSIS Act,* whose principal purpose is to reduce a threat to the security of Canada as defined in s. 2 of the *CSIS Act*."[94]

(U) These measures are subject to specific stipulations. Section 12.1 of the *CSIS Act* states that CSIS may only undertake a TRM if there are reasonable grounds to believe (RGB) that the identified conduct is a threat to the security of Canada.[95] TRMs must be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat, and the reasonably foreseeable effects on third parties, including on their right to privacy. CSIS must also consult with other federal departments, where appropriate, with respect to whether they may be in a position to reduce the threat. Finally, CSIS must seek a warrant from a judge where a proposed TRM would limit a right or freedom guaranteed by the *Charter* or would otherwise be contrary to Canadian law.

(S) In addition to these statutory requirements, the 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* require all TRMs to undergo a four-pillar risk assessment that examines the operational, reputational, foreign policy, and legal risks of proposed actions on a scale of low, medium or high. Moreover, they require that, when assessing the appropriate means of reducing a threat, CSIS consider the range of other possible national security tools available to the broader community, and consult with departments and agencies of the Government of Canada with mandates or authorities closely related to the proposed TRM. It is also important to note that both MDs operate concurrently: the 2015 MD section regarding Operations remains in effect, whilst the section concerning Accountability in the 2015 MD is superseded by the 2019 MD.

---

[92] *Anti-terrorism Act,* SC 2015, c 20.

[93] Among other things, CSIS cannot engage in measures that cause death or bodily harm, subject an individual to torture, or detain or violate the sexual integrity of an individual: *CSIS Act,* RSC 1985, c C-23, ss 12.1 and 12.2.

16(1)(b) [94] CSIS, "[redacted]

[95] *R v Kang-Brown*, [2008] 1 SCR 456. Reasonable suspicion requires only a partial or confirmed belief, but still one that is reasonable and based on some evidence. Reasonable grounds to believe, however, refers to the point where reasonable probability replaces suspicion and mere possibility. Reasonable grounds to believe is a higher evidentiary standard based on information that is relevant, current, accurate, precise, compelling, and reliable. That TRMs are subject to RGB and not RGS is noteworthy, and reflects the relatively higher intrusiveness of such measures as compared to pure intelligence collection.

ANNEX C: CASE SELECTION STRATEGY

(S) NSIRA's population for case selection were the [redacted] TRMs – all those implemented in the calendar year 2021 – laid out in Table 1 [redacted]

(TS) TABLE 1: ALL TRMS IMPLEMENTED IN 2021

TRM	Dates of Implementation	Threat Type
[redacted]		

15(1)(d)(ii)

[redacted]

(S) Of these 21 cases, three were TRMs *first* implemented in 2020, with subsequent implementations during the review period.[96] [redacted][97] As such, and given the desire to examine the full lifecycle of the TRM within the specified review period, NSIRA dropped [redacted]

(S) [redacted]

[96] These were [redacted]
[97] For example, a TRM first implemented in 2020 with subsequent implementations in 2021 would be counted among the number of implementations in 2020 and not be included in the same statistic for 2021.

prevalence and importance of measures aimed at reducing threats defined under subsection 2c of the *CSIS Act*. These threats include, but are not limited to, those stemming from RMVE and IMVE. As noted in paragraph 34 of the report, since 2015, 2c threats have been the most frequently subject to TRMs (as compared to other threats described by the *Act*), and will likely continue to be a focus in the years to come.[98] As such, NSIRA judged that any findings and/or recommendations emerging from the review of TRMs aimed at 2c threats would be useful to CSIS going forward, as similar TRMs are contemplated, designed, proposed and implemented.

(TS//CEO) [redacted].[99] NSIRA reviewed documentation associated [redacted][100]).

(S) For these reasons, [redacted] was dropped from the sample, leaving three TRMs for review (n=3).

[98] In addition to CSIS's 2021-2023 Intelligence Priorities, see also testimony on the "Rise of Ideologically Motivated Violent Extremism in Canada" delivered before the Standing Committee on Public Safety and National Security (SECU) on 31 March 2022 (https://ourcommons.ca/DocumentViewer/en/44-1/SECU/meeting-16/notice).

[99] N.B., [redacted]

[100] SIRC's 2016 TRM review noted the challenges associated with documenting strategic outcomes which are difficult to quantify (such as reducing the "ability" or "influence" of threat actors), and recommended that CSIS "consider the realistic prospects of both measuring and achieving the strategic outcomes." CSIS agreed with the recommendation, and committed to "actively working to ensure threat reduction outcomes are more quantifiable." SIRC Annual Report 2016-2017, p. 26. NSIRA recognizes the effort that CSIS has made in this direction since 2016, which is reflected in the strategic outcomes articulated [redacted] Nonetheless, it remains the case that certain measures by their nature will be more challenging than others in terms of documenting outcomes. For practical purposes, such challenges with respect [redacted] were prohibitive vis-à-vis the goals of the review.