



**REVIEW OF CSIS THREAT REDUCTION ACTIVITIES:
A Focus on Information Disclosure to External Parties**

(NSIRA REVIEW 2021-04)

Table of Contents

- I EXECUTIVE SUMMARY 2**
- II AUTHORITIES 3**
- III INTRODUCTION..... 3**
 - Background 3
 - Scope 3
 - Sources and Methodology 3
 - TRM mandate..... 4
 - Governance..... 5
- IV FINDINGS AND RECOMMENDATIONS 6**
 - Brief overview - TRMs, by the numbers 6
 - CSIS’s information disclosures as part of TRMs 7
 - Types of external parties involved in proposed TRMs 7
 - Nature of information disclosed..... 9
 - Identification, documentation and consideration of impacts10
 - Measures affecting [REDACTED] 11
 - Measures affecting [REDACTED] 13
 - Measures [REDACTED] 14
 - Measures [REDACTED] 15
 - Identification of impacts 17
 - Documentation of outcomes 18
 - Consideration of impacts when assessing whether a warrant is required 19
- V CONCLUSION 21**
- VI ANNEX A: FINDINGS and RECOMMENDATIONS 23**

I EXECUTIVE SUMMARY

1. **[REDACTED]** This is the second annual review of the Canadian Security Intelligence Service's (CSIS) threat reduction measures (TRMs) completed by the National Security Intelligence Review Agency (NSIRA). This review sought to expand upon findings from last year's review by examining a larger number of TRMs wherein CSIS disclosed information to external parties with their own levers of control, to reduce identified threats.
2. **[REDACTED]** The review studied the characteristics of these particular TRMs but focused its examination upon the extent to which CSIS appropriately identified, documented and considered any plausible adverse impacts that these measures could have on affected individuals.
3. **[REDACTED]** With respect to the TRMs studied, NSIRA observed that **[REDACTED]** of external parties were involved in these TRMs, **[REDACTED]** which had varied levers of control with which they could take action against identified threats or the subjects of these measures. NSIRA also observed that CSIS disclosed different kinds of information to external parties for these TRMs. NSIRA noted that CSIS's documentation of TRMs was uneven. CSIS did not always document **[REDACTED]** sometimes excluded an account of the actions taken by external parties as part of these measures. NSIRA also noted that CSIS documentation of the information it disclosed to external parties, as part of these TRMs, was inconsistent, and at times, lacked clarity and specificity.
4. **[REDACTED]** An understanding of both external parties' levers of control and the scope and breadth of information disclosed to external parties for TRMs is important and feeds into the overall risk assessment of each proposed measure. Without more robust documentation, CSIS is neither capable of assessing the efficacy of its measures nor appreciating the full impact of its actions on the subjects of its measures.
5. **[REDACTED]** In 2020, NSIRA asserted that, when determining whether a warrant is required, CSIS should consider impacts on individuals resulting from the entirety of threat reduction measures: both from CSIS's disclosure of information and from actions taken by recipient external parties, to reduce the threat. The adverse impacts on individuals observed in the TRMs examined for this year's review underscore NSIRA's position.
6. **[REDACTED]**
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
7. **[REDACTED]** The current assessment framework **[REDACTED]** to determine whether a warrant is required is overly narrow and does not sufficiently consider the full impacts of CSIS threat reduction measures. NSIRA recommends that CSIS consider plausible adverse impacts resulting not only from CSIS disclosures of information but also from the actions of external parties as part of TRMs, when determining whether a warrant is required.

8. **[REDACTED]** NSIRA was able to use its direct access to CSIS information repositories to confirm information that it needed to verify and to pursue necessary additional inquiries. For that reason, NSIRA has a high level of confidence in the information on which it relied to complete this review. NSIRA would also like to recognize that CSIS was timely in responding to NSIRA's requests for information throughout the course of this review.

II AUTHORITIES

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

III INTRODUCTION

Background

10. **[REDACTED]** This review is the second annual review of CSIS threat reduction measures (TRMs) completed by the National Security Intelligence Review Agency (NSIRA).¹
11. **[REDACTED]** In its first review of TRMs (NSIRA's 2020 review), NSIRA examined **[REDACTED]** TRMs in which CSIS disclosed information to an external party.² In all cases examined, CSIS disclosed the information to an external party in order for the external party to take action in some way using its own levers of control to address the identified threat.³ This year's review examined a larger subset of TRMs that involved CSIS disclosing information to an external party for the purpose of obtaining a desired threat reduction outcome. NSIRA focused primarily on examining how CSIS identifies and considers the plausible adverse impacts of these measures on affected individuals.

Scope

12. **[REDACTED]** The review period covers June 18, 2015 to December 31, 2020, and includes **[REDACTED]** proposed TRMs that involved CSIS disclosing information to an external party for the purpose of using that external party as a conduit for the desired action against the subject of the TRM.⁴ Of these **[REDACTED]** proposed TRMs, **[REDACTED]** were approved and **[REDACTED]** were implemented.

Sources and Methodology

13. **[REDACTED]** NSIRA examined information from a variety of sources, including:

¹ NSIRA's predecessor, the Security Intelligence Review Committee (SIRC), examined CSIS's use of threat reduction measures between 2016 and 2019.

² NSIRA, *Review of CSIS Threat Reduction Activities* (No. 2020-05), May 2020.

³ These **[REDACTED]** TRMs involved CSIS disclosing information to an external party **[REDACTED]** for the principal purpose of reducing a security threat. The specific goal of these TRMs was for the external parties to take action, **[REDACTED]**

[REDACTED] ultimately reducing the threat that CSIS had identified. NSIRA, *Review of CSIS Threat Reduction Activities* (No. 2020-05), May 2020, pg. 5.

⁴ On June 18, 2015, CSIS received its threat reduction mandate under the *Anti-Terrorism Act, 2015*.

Document Review

- Ministerial directions issued by the Minister of Public Safety and Emergency Preparedness to CSIS.
- CSIS's internal governance framework for TRMs, which included policies, procedures, guidance and training material, tracking systems and cooperation agreements.
- All pertinent threat reduction measure documentation, email communications, operational messages, and
- Relevant , including responses to NSIRA's Requests for Information.

Briefing

- One briefing from the Department of Justice.⁵

Analysis of Administrative Data

- Descriptive statistics of the TRM sample.
- Cross-reference of TRM subjects in the review sample with NSIRA's investigation files for complaints submitted to SIRC (2015 to July 2019) and NSIRA (July 2019 to 2020) in order to document any complaints investigations underpinned by a CSIS TRM.

TRM mandate



14. 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.⁶ The new measures represented an unprecedented departure from CSIS's traditional intelligence collection role.
15. In July 2019, the *National Security Act, 2017*, came into force and 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)*. They included specific provisions affirming the need for all TRMs to comply with the *Charter*, and stipulating that measures could only limit *Charter* rights or freedoms if authorized by a judge under a warrant. The amendments also included an expanded list of prohibited conduct under the TRM regime: 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.⁷
16. The *CSIS Act* does not provide a precise definition of "measures to reduce the threat." As such, CSIS has developed its own definition to guide its TRM activities. According to CSIS, a TRM is "[a]n operational measure undertaken by the Service,

⁵ Justice briefing for NSIRA, October 18, 2021. Previous briefings, conducted over the course of the NSIRA 2020 review were also considered.













⁶ *Anti-terrorism Act*, SC 2015, c. 20.

⁷ SC 2019, c.13; *CSIS Act*, sections 12.1 and 12.2.



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*.⁸

17.  Section 12.1 of the *CSIS Act* states that CSIS may only undertake a TRM if there are reasonable grounds to believe that the identified conduct is a threat to the security of Canada. 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. CSIS must also 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.
18.  The 2015 *Ministerial Direction for Operations and Accountability* and the 2019 *Ministerial Direction for Accountability* issued by the Minister of Public Safety require all TRMs to undergo a four-pillar risk assessment that examines the operational, political, foreign relations, and legal risks of proposed actions on a scale of low, medium or high. In addition, 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.

Governance

19.  CSIS's TRM unit is made up of  full-time employees, and is responsible for developing and updating policies and procedures related to TRMs; it also provides support to operational units involved with TRMs.
20.  Operational units must consult with the TRM unit at the planning stage, and while drafting 




21.  CSIS's governing policy outlines the requirements associated with planning, approving, implementing, and reporting TRMs, including their use in exigent circumstances.⁹ The policy replicates the relevant provisions of the *CSIS Act*, without adding much direction beyond citing the existing legislative regime. For example, the policy incorporates the Act's requirement to ensure that TRMs are reasonable and proportional, 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 of the measure on third parties, including their right to privacy.¹⁰ 



⁸ CSIS, "Introduction of Threat Reduction Activities" 

⁹ The TRM governance suite also included a template and guidelines for the TRM Request for Approval (RFA), 
 Also available were guidelines addressing frequently asked questions related to TRM process and approvals, consultation and assistance and implementation.

¹⁰ CSIS, *Conduct of Operations, section 12.1 Threat Reduction Measures*, Version 4, paras. 3.1, 3.4 and 3.5.

22. [REDACTED]

23. [REDACTED] NSIRA notes that in conducting its legal assessments, [REDACTED]

24. [REDACTED] CSIS has also developed internal guidelines for consultations with other government departments, [REDACTED]

IV FINDINGS AND RECOMMENDATIONS

Brief overview - TRMs, by the numbers

26. [REDACTED] During the review period, CSIS proposed [REDACTED] TRMs in total.¹⁴
- [REDACTED] proposed measures involved an external party that had an ability to act using its own levers of control.¹⁵
 - Of these [REDACTED] proposed measures, [REDACTED] were approved and [REDACTED] implemented.
 - Of the [REDACTED] approved measures, none of them, in CSIS’s view, required judicial authorization, or warrants, to proceed.

[REDACTED] *Figure 1: Life cycle of TRMs involving an external party that had levers of control* [REDACTED]

¹¹ CSIS consults with [REDACTED]

¹² CSIS, “How to Complete a Request for Approval,” *Conduct of Operations, section 12.1 Threat Reduction Measures*, [REDACTED]

¹³ CSIS, *Conduct of Operations, section 12.1 Threat Reduction Measures*, [REDACTED]

¹⁴ This total does not include [REDACTED]

¹⁵ CSIS maintains three broad categories of TRMs: messaging, leveraging and interference. According to CSIS, leveraging involves providing threat information to private companies for them to take action, at their discretion and pursuant to their authorities, to impede a person’s ability to obtain services. [REDACTED]

[REDACTED] NSIRA reviewed all TRMs proposed between 2015 and 2021.

27. [REDACTED] Comprising [REDACTED] proposed measures, information disclosure to external parties was a common strategy that CSIS proposed as part of TRMs, to reduce perceived threats to the security of Canada.

CSIS's information disclosures as part of TRMs

28. [REDACTED] NSIRA examined documentation supporting the [REDACTED] proposed TRMs, including the [REDACTED] implemented TRMs where CSIS disclosed information to an external party to reduce a threat to the security of Canada. NSIRA looked to identify and assess:
- the types of external parties involved in the proposed TRMs;
 - the nature of the information that CSIS shared as part of these measures; and
 - the extent to which CSIS identified, documented and considered the plausible adverse impacts of the measure on individuals.

Types of external parties involved in proposed TRMs

29. [REDACTED] NSIRA provides examples of the types of external parties involved in proposed TRMs, as well as some of the varied actions they could take in Table 1, below.

Table 1: Proposed TRMs [REDACTED] by type of external party, intended outcomes, and TRM status.

Type of External Party	Intended Outcome(s)	TRM Status	Observations
------------------------	---------------------	------------	--------------

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
------------	------------	------------	------------

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

direct and indirect impacts may be difficult to ascertain with any precision. This affects the rigour of any associated risk assessment, including the legal risk assessment.

34. [REDACTED] By contrast, NSIRA noted certain instances in which CSIS provided a sufficiently detailed description of the information to be disclosed in its documented materials. [REDACTED]

35. [REDACTED] In NSIRA's view, the precise content, including the scope and breadth of the information to be disclosed to an external party as part of a TRM, is important and feeds into the overall risk assessment of the proposed measure. A detailed and precise description of the information to be disclosed would allow for more considered assessments.

36. [REDACTED] **Finding 1: NSIRA finds that CSIS's documentation of the information disclosed to external parties as part of TRMs was inconsistent and, at times, lacked clarity and specificity.**

37. [REDACTED] **Recommendation 1: NSIRA recommends that when a TRM involves CSIS disclosing information to external parties, CSIS should clearly identify and document the scope and breadth of information that will be disclosed as part of the proposed measure.**

Identification, documentation and consideration of impacts

38. [REDACTED] NSIRA's 2020 TRM review examined [REDACTED] TRMs where CSIS disclosed information to an external party in order to disrupt a [REDACTED] threat actor.³¹ That review underlined the importance of considering all plausible adverse impacts on an affected individual as part of the TRM approval process. In this year's review, NSIRA sought to examine a larger sample of TRMs in which CSIS disclosed information to external parties to reduce an identified security threat. This year's review allowed NSIRA to gain greater insight into CSIS' intended outcomes for these TRMs and how CSIS assessed their impact on the individual.

39. [REDACTED] The following examples highlight common impacts that NSIRA identified:

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

³¹ NSIRA, *Review of CSIS Threat Reduction Activities* (No. 2020-05), May 2020.

[REDACTED]

[REDACTED]

- 40. [REDACTED] The interests engaged where measures affect [REDACTED] can have significant and lasting impacts on the subjects and their families. For example, measures that impact the [REDACTED] interfere with [REDACTED]. Moreover, the associated hardships can affect the subject's inherent dignity. The norms of our liberal democracy dictate that people in society should be able to [REDACTED]. When CSIS is assessing the reasonableness and proportionality of TRMs that can impact the [REDACTED] as well as assessing whether a warrant is required, it is important that the analysis sufficiently take these factors into consideration.

Measures affecting [REDACTED]

[REDACTED]

- 41. [REDACTED]

- 42. [REDACTED]

- 43. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

44. [REDACTED] In NSIRA's view, the identification and assessment of the risks associated with [REDACTED] [REDACTED] failed to fully explore the plausible adverse impacts of these actions. [REDACTED]

[REDACTED]

45. [REDACTED]

46. [REDACTED]

[REDACTED]

47. [REDACTED]

[REDACTED]

[REDACTED]

48.

[REDACTED]

49.

[REDACTED] Nevertheless, NSIRA observes that CSIS approved a TRM without knowing the actions, if any, that the [REDACTED] was required to take under Canadian law or could take, pursuant to its [REDACTED]. This information could have contributed to the assessment of the plausible adverse impacts of the measure upon individuals. [REDACTED]

Measures affecting [REDACTED]

[REDACTED]

50.

[REDACTED]

51.

[REDACTED]

[REDACTED]

[REDACTED]

- 52. [REDACTED]

[REDACTED]

- 53. [REDACTED]

- 54. [REDACTED] NSIRA notes that, at the time the proposed measure was assessed, CSIS did not appreciate the authority and capacity of each of the organizations to prevent the individual from [REDACTED]

Measures preventing [REDACTED]

[REDACTED]

- 55. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

56. [REDACTED]

Measures [REDACTED]

[REDACTED]

57. [REDACTED]

58. [REDACTED]

[REDACTED]

[REDACTED]

59. [REDACTED] While this TRM likely raises issues associated with the extraterritorial application of the *Charter*, NSIRA focused its assessment on the scope and nature of the plausible adverse impacts of the measure. NSIRA notes that at the time the proposed measure was assessed, CSIS did not have a developed understanding of potential harms [REDACTED]

[REDACTED]

[REDACTED]

60. [REDACTED]

61. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

62. [REDACTED]

63. [REDACTED]

64. [REDACTED]

Identification of impacts

65. [REDACTED] NSIRA observes that CSIS's understanding of the scope and breadth of the potential ramifications of disclosing information to external parties varied across the reviewed sample. NSIRA expected to see that when CSIS disclosed information to an external party, CSIS had a genuine appreciation of the scope of the plausible adverse outcomes, including the actions that the external party could take. NSIRA also expected to see a consideration of, not only the impacts of the intended outcomes of the measure, but also any collateral adverse impacts.

66. [REDACTED] For example, [REDACTED] NSIRA expected CSIS to understand the ability of the external party to take action. As noted in some of the examples above, while CSIS always had a clear desired outcome for the TRM, CSIS did not always have an adequate appreciation of the powers and authority (levers of control) of the external party receiving the information.

67. [REDACTED] NSIRA observed that CSIS had turned its mind to whether the proposed measure could have [REDACTED] However, the [REDACTED]

[REDACTED]

identified impacts fell short because they did not consider the foreseeable possibility that the individual could be [REDACTED]

68. [REDACTED] **Finding 2: NSIRA finds that CSIS does not systematically identify or document the external parties' authority and ability to take action, or plausible adverse impacts of the measure.**

69. [REDACTED] **Recommendation 2: NSIRA recommends that CSIS fully identify, document and consider the authority and ability of the external party to take action, as well as the plausible adverse impacts of the measure.**

Documentation of outcomes

70. [REDACTED] NSIRA expected to obtain more certainty with respect to the outcomes of these measures by reading official outcomes reports, [REDACTED]
[REDACTED]
[REDACTED] This suggested that CSIS's reporting system was inadequate or that these reports were improperly filed or non-existent.⁶³

71. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

72. [REDACTED] NSIRA observes that follow-ups with the external party should be an essential component of measures involving information disclosure whose principal purpose is to reduce a security threat. Without robust documentation and after action reports on TRMs, CSIS is incapable of assessing the efficacy of the measure as well as appreciating the full impact of its actions. An examination of well-documented after action reports will also enable CSIS [REDACTED] to determine whether their initial reasonableness and proportionality assessment may have failed to consider important considerations, which can, in turn, inform the assessments of future proposed TRMs.

73. [REDACTED] **Finding 3: NSIRA finds that CSIS did not consistently document the outcomes of TRMs in accordance with its policy. Furthermore, CSIS policy does not require it to document the actions taken by external parties.**

74. [REDACTED] **Recommendation 3: NSIRA recommends that CSIS should amend its TRM policy to include a requirement to systematically document the outcomes of TRMs, including actions taken by external parties. This practice should inform post-action assessments and future decision-making.**

⁶³ NSIRA notes that in the early years of the TRM program, outcome reporting was not required, however SIRC reviews of CSIS TRM activities as well as a CSIS internal audit both highlighted the need for after action reporting. Since this time, CSIS has formalized outcome reporting as part of the TRM process.

⁶⁴ CSIS, *Frequently Asked Questions*, version 3, 2019.

75. **[REDACTED] Recommendation 4: NSIRA recommends that CSIS comply with its record-keeping policies related to documenting the outcomes of TRMs.**

Consideration of impacts when assessing whether a warrant is required

76. **[REDACTED]** The variety of impacts observed in this year’s TRM review highlights the salience of NSIRA’s recommendation in 2020, namely that CSIS consider more comprehensively potential adverse impacts of these types of measures on the affected individuals. This recommendation underlined that all potential impacts on an affected individual, even where they are carried out by the external party and not CSIS, should be considered when determining whether a warrant is required.⁶⁵

77. **[REDACTED]**
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

78. **[REDACTED]** This limited consideration of the impacts of TRMs was also evident in this year’s review. **[REDACTED]**
[REDACTED]

79. **[REDACTED]** In an October 2021 briefing between NSIRA and **[REDACTED]**
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

80. **[REDACTED]**
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

⁶⁵ NSIRA, *Review of CSIS Threat Reduction Activities* (No. 2020-05), May 2020.
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- [REDACTED]**
[REDACTED]
[REDACTED]
[REDACTED]
81. **[REDACTED]** NSIRA notes that CSIS cannot avoid responsibility just because the outcomes of an action would be effected by someone else's hand. **[REDACTED]**
[REDACTED]
[REDACTED] Where there is a sufficient causal connection between CSIS's actions and the ultimate outcomes, the principles of fundamental justice apply to deprivations of life, liberty or security effected by external parties.⁷² **[REDACTED]**
[REDACTED] This is particularly so when such a foreseeable risk has been identified in the reasonableness and proportionality analysis.
82. **[REDACTED]** The current structure used to determine whether CSIS should obtain a warrant for its TRMs is an insufficient implementation of the warrant requirements of the TRM provisions. Sections 12.1 (3.2) and (3.4) require CSIS to seek a warrant when the measure would limit a *Charter* right or otherwise be contrary to Canadian law. The current **[REDACTED]** by CSIS is overly narrow and should not be based on the impacts of a CSIS action alone. Rather, it should consider the full impact of the measure, including any direct and indirect impacts caused or initiated by external parties.
83. **[REDACTED]** The *CSIS Act* is clear that when a proposed TRM would limit a *Charter* right or freedom, or would otherwise be contrary to Canadian law, CSIS must seek a judicial warrant. In NSIRA's 2020 TRM Review, CSIS deemed that a warrant was not required for the reviewed TRMs, because it viewed the external party as responsible for taking action, not CSIS. NSIRA identified its concerns with this approach, and noted that consideration of the full impact of such proposed TRMs, including any downstream *Charter* implications resulting from the external parties' actions could require CSIS to obtain a warrant before undertaking these types of measures.
84. **[REDACTED]** CSIS's response to this recommendation stated "the Department of Justice will further consider this recommendation and factor it into its work related to TRM under the *CSIS Act*."⁷³
85. **[REDACTED]** However, as noted above, **[REDACTED]**
[REDACTED]
[REDACTED]
[REDACTED]
86. **[REDACTED]** NSIRA fundamentally disagrees with CSIS's understanding of and approach to the legal analysis of determining whether a warrant is required for proposed TRMs.
87. **[REDACTED]** Going forward, NSIRA expects that when proposing a TRM where an individual's *Charter* rights would be limited, or that would otherwise be contrary to Canadian law,

⁷¹ Justice, LRA for 2017-09, February 21, 2017.

⁷² *Suresh v. Canada (Minister of Citizenship and Immigration)*, [2002] 1 SCR 3 at para 54.

⁷³ NSIRA, 2020 Annual Report, page 62.

whether at the direct hand of CSIS or that of an external party to whom CSIS disclosed information, CSIS will seek a warrant to authorize the TRM.

88. **■ Finding 4: NSIRA finds that when determining whether a warrant is required, CSIS's assessment is overly narrow due to a failure to appropriately consider the impacts resulting from external party actions.**
89. **■ Recommendation 5: NSIRA recommends that CSIS appropriately consider the impacts resulting from external party actions when determining whether a warrant is required.**

V CONCLUSION

90. **■** The variety of impacts observed in this year's review, combined with the gaps identified in CSIS's understanding and assessment of these impacts highlights the salience of a number of NSIRA's recommendations in 2020.
91. **■** The TRM regime was introduced in 2015 to address an evolving security and intelligence landscape. NSIRA recognizes that CSIS' threat disruption powers can be an effective tool to diminish a national security threat. While these powers provide CSIS with additional flexibility, they also demand heightened responsibility, given their covert nature and ability to profoundly impact, not only the subject of a given TRM, but others potentially captured by its scope. As this review demonstrates, TRMs can interfere with

 Mindful of the need to reduce threats, but recognizing the competing values at stake, it is critical that CSIS subject its TRMs to robust and thorough analyses, both prior to and following their implementation.
92. **■** NSIRA reiterates its recommendation that CSIS consider more comprehensively the plausible adverse impacts of these types of measures on the affected individuals, even when they are carried out by the external party and not CSIS. These impacts should be considered not only when considering the reasonableness and proportionality of a proposed measure, but also when determining whether a warrant is required.
93. **■** In addition, this year's review again highlighted the importance of Justice's involvement in the TRM approval process. More specifically, the necessity for Justice to be provided sufficient information, in this case on the nature of the information to be disclosed by CSIS as well as the authority and actions (levers of control) the external party can take, to allow Justice to provide considered legal advice.
94. **■** Finally, without robust documentation and after action reports on TRMs, CSIS is incapable of assessing the efficacy of the measures or appreciating the full impact of its actions. CSIS should systematically identify the actions that are taken by external parties for threat reduction measures that involve CSIS disclosures of information. Identifying and recording these actions and the subsequent impacts on TRM subjects will inform not only TRM risk assessments, but also enable CSIS to build upon its experience with TRMs and guide future decision-making.
95. **■** While outside of the scope of this review, NSIRA is aware that in January 2021, CSIS launched

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] NSIRA may in the future review [REDACTED] and whether it has impacted the identification and consideration of plausible adverse impacts of measures on individuals.

VI ANNEX A: FINDINGS and RECOMMENDATIONS

■ **Finding 1:** NSIRA finds that CSIS's documentation of the information disclosed to external parties as part of TRMs was inconsistent and, at times, lacked clarity and specificity.

■ **Finding 2:** NSIRA finds that CSIS does not systematically identify or document the external parties' authority and ability to take action, or plausible adverse impacts of the measure.

■ **Finding 3:** NSIRA finds that CSIS did not consistently document the outcomes of TRMs in accordance with its policy. Furthermore, CSIS policy does not require it to document the actions taken by external parties.

■ **Finding 4:** NSIRA finds that when determining whether a warrant is required, CSIS's assessment is overly narrow due to a failure to appropriately consider the impacts resulting from external party actions.

■ **Recommendation 1:** NSIRA recommends that when a TRM involves CSIS disclosing information to external parties, CSIS should clearly identify and document the scope and breadth of information that will be disclosed as part of the proposed measure.

■ **Recommendation 2:** NSIRA recommends that CSIS fully identify, document and consider the authority and ability of the external party to take action, as well as the plausible adverse impacts of the measure.

■ **Recommendation 3:** NSIRA recommends that CSIS should amend its TRM policy to include a requirement to systematically document the outcomes of TRMs, including actions taken by external parties. This practice should inform post-action assessments and future decision-making.

■ **Recommendation 4:** NSIRA recommends that CSIS comply with its record-keeping policies related to documenting the outcomes of TRMs.

■ **Recommendation 5:** NSIRA recommends that CSIS appropriately consider the impacts resulting from external party actions when determining whether a warrant is required.