REVIEW OF CSIS THREAT REDUCTION ACTIVITIES

(NSIRA REVIEW 2020-05)

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *1-833* 890-0293 Fax: *613* 907-4445

Contents

I EXECUTIVE SUMMARY

1. 2020 marks five years since the Canadian Security Intelligence Service (CSIS) was granted the authority to undertake threat reduction measures (TRMs) under the *Anti-terrorism Act, 2015*. This was a substantial change to CSIS's mandate, which had been limited to collecting information and advising government on threats to the security of Canada. Pursuant to subsection 8(2) of the *National Security and Intelligence Agency Act* (*NSIRA Act*), the National Security and Intelligence Review Agency (NSIRA) is required to review annually at least one aspect of CSIS's performance in using its threat reduction powers.

2. This is NSIRA's first review of CSIS's threat reduction mandate. It includes a detailed compliance review of a sample of TRMs from 2019. The review also contains a high-level analysis of CSIS's use of threat reduction measures over the past five years to identify trends and to inform NSIRA's choice of future review topics.

3. The sample reviewed by NSIRA consisted of TRMs that were employed to disrupt the threat posed by hostile foreign states to Canadian democratic institutions. NSIRA selected these TRMs as they were approved in the context of the 2019 federal election and so they were both timely and topical. NSIRA assessed the measures against legislative and policy requirements, as well as Ministerial Direction.

4. For all of the measures reviewed, NSIRA finds that CSIS met its obligations under Ministerial Direction, namely that CSIS consult with its government partners and complete an assessment of the operational, political, foreign relation and legal risks of each TRM.

5. NSIRA's legal assessment of the TRMs focused on the requirements in the *CSIS Act* that CSIS have "reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada" and that the measure be "reasonable and proportional in the circumstances".[1] In making its assessment, NSIRA was attentive to the advice provided CSIS by the Department of Justice's National Security Litigation and Advisory Group (NSLAG).

7. For most of the measures taken by CSIS, NSIRA observes that the measures satisfied the requirements of the *CSIS Act*. NSIRA also observes, however, that in a limited number of cases, In particular, CSIS selected individuals without a rational link between the selection of the individual and the threat. As a result, these measures were not "reasonable and proportional" as required under the *CSIS Act*.

[1] *CSIS Act,* subsection 12.1(1).

8. For one type of TRM,

NSIRA is of the view that more consideration needs to be given to the possible existence of an between CSIS and third parties acting at CSIS's behest. Such a relationship would require CSIS to consider fully the *Canadian Charter of Rights and Freedoms* (*Charter*) implications of its measures, and could require CSIS to obtain warrants before taking certain measures.

9. Finally, NSIRA noted some inconsistencies in the type of information provided to decision-makers in its internal requests for approval. NSIRA also finds gaps and inconsistencies in CSIS's documentation; these hindered NSIRA's compliance review. As a result, NSIRA recommended that formalized and documented processes be developed for the management of all TRM-related information. In addition, NSIRA recommended that all pertinent facts pertaining to the TRM be formally provided to NSLAG to ensure that NSLAG has the information necessary to provide considered legal advice.

10. The legal issues and questions raised in this review, as well as our analysis of trends across the five years, point the way to further reviews by NSIRA. In particular, NSIRA was struck by the potential for TRMs where CSIS works with third parties to affect rights and freedoms protected under the *Charter*. In future, NSIRA will pay particular attention to this class of TRMs and the associated legal risks. NSIRA also notes that CSIS has yet to undertake a TRM under the authority of a court warrant. If and when CSIS obtains a TRM warrant, NSIRA will prioritize it for review.

II AUTHORITIES

11. This review was conducted under the authority of subsection 8(2) of the *NSIRA Act*,[2] which requires NSIRA, each calendar year, to review at least one aspect of CSIS's performance in taking measures to reduce threats to the security of Canada.

III INTRODUCTION

Review background and structure

12. This review marks five years since CSIS was granted authority to undertake threat reduction measures (TRMs) under the *Anti-terrorism Act, 2015*.[3] It is also NSIRA's first review of these measures. Prior to the creation of NSIRA, the Security Intelligence Review Committee (SIRC) was responsible for this annual review.[4] The last of SIRC's four TRM reviews was published in January 2019.[5]

[2] *National Security and Intelligence Review Agency Act*, SC 2019, c. 13 ss. 8(2).
[3] *Anti-terrorism Act,* SC 2015, c. 20.
[4] Section 38 (1.1) of the *CSIS Act,* legislated SIRC to review "at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada".
[5] See SIRC reviews 2015-07, 2016-09, 2017-16 and 2018-06. SIRC also reviewed CSIS disruption measures in 2010 as part of SIRC Review 2009-05.

13. NSIRA's first annual TRM review set out to:

a) fulfill its obligation to examine one aspect of CSIS's use of its threat reduction powers through a compliance review of a sample of TRMs; and

b) establish a comprehensive record of CSIS's TRMs since 2015.

14. The review comprises two main sections. The first is a detailed compliance review of a specific set of TRMs from 2019 that focused on threats posed by hostile foreign states to Canadian democratic institutions.[6] This sample was considered timely and relevant given public interest in the threat of foreign influenced activities.[7] The TRMs under review also constitute CSIS's first use of it threat reduction powers to disrupt threats in the context of an election.

15. The review assessed the measures taken against the requirements in the *CSIS Act*[8] as well as Ministerial Direction and CSIS's policies and procedures for the implementation of a TRM.

16. The second section of the review consists of an annex containing an analysis of CSIS's use of threat reduction measures over the past five years[9] in order to identify trends, gaps and emerging issues of relevance to NSIRA. This work will help inform NSIRA's choice of future TRM review topics.[10] NSIRA remains up-to-date regarding CSIS's use of these powers by virtue of CSIS's requirement, under subsection 12.1(3.5) of the *CSIS Act*, to provide notification to NSIRA of threat reduction measures taken.

History of TRM powers

17. In June 2015, the enactment of the *Anti-terrorism Act, 2015* 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.[11]

18. This represented a substantial change to CSIS's primary mandate, which, until then, had been limited to the collection and analysis of information and intelligence, and reporting to and advising the Government of Canada (GoC) on threats. Although other departments and agencies could use information provided by CSIS to deal with threats under their own authorities, prior to the legislative change, the *CSIS Act* did not explicitly authorize CSIS to take direct action on its own information against threats.

19. The appropriateness of granting CSIS the authority to reduce threats to national security was publicly criticised and debated. Of concern was the potential for CSIS TRMs to

---

TRMs formed the core compliance sample.

NSIRA reviewed additional TRMs for comparison purposes. See Annex B for more details.

[7] Alex Boutilier, Craig Silverman, Jan Lytvynenko, "Canadian Spies Given New 'Disruption' Powers to Combat Foreign Influence in Elections", *The Toronto Star* (July 4, 2019).

[8] *CSIS Act*, RSC, 1985, c C-23.

[9] See Annex B for additional details on the development of the comprehensive record of CSIS TRM activities.

[10]

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

violate the rights and freedoms of Canadians. The lack of clarity regarding the limits of CSIS's new powers raised questions regarding whether CSIS could capture, detain, interrogate and render individuals. The potential for CSIS threat reduction activities to interfere or undermine police investigations or prosecutions was also cited as a concern.

20. Four years later, in July 2019, the *National Security Act, 2017*[12] came into force and, with it, amendments to section 12.1 and other related sections of the *CSIS Act*. These amendments explicitly prohibited certain activities, conferred on CSIS an obligation to consult other government departments prior to undertaking a measure, and emphasized that threat reduction measures taken by CSIS must comply with the *Charter*.[13]

What is a TRM?

21. The *CSIS Act* does not provide a precise definition of "measures to reduce the threat." As such, CSIS has developed an internal definition to guide those activities. According to CSIS policy, a TRM is:

> [a]n operational measure undertaken by the Service, 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*.[14]

22. A TRM must be purposeful, or in other words, it is an action taken for the express purpose of reducing a threat, rather than simply the unintended consequence of an action taken under a different section of the *CSIS Act*.[15]

23. CSIS identifies three broad categories of TRMs: messaging, leveraging, and interference. According to CSIS:

a) "Messaging"

b) "Leveraging"

c) "Interference"

[12] SC 2019, c.13.
[13] *CSIS Act,* sections 12.1 and 12.2.
[14] Introduction of Threat Reduction Activities
[15] Introduction of Threat Reduction Activities
[16]

Legislative and ministerial requirements

24. The *CSIS Act* authorizes threat reduction measures by CSIS if there are "reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada."[18] TRMs must also be reasonable and proportional in the circumstances.[19]

25. CSIS must seek a judicial authorization (a warrant) where a proposed TRM would limit a right or freedom guaranteed by the *Charter* and/or be contrary to any Canadian law.[20] CSIS must also consider the availability of other means to reduce the threat and consult with other federal departments, where appropriate, as to whether those departments are in a position to reduce the threat.[21]

26. Finally, the 2015 Ministerial Direction for Operations and Accountability and the 2019 Ministerial Direction for Accountability require TRMs to undergo a four-pillar risk assessment that examines the operational, political, foreign relations and legal risks of the proposed action. In addition, when assessing the appropriate means of reducing a threat, CSIS is required to consider the range of possible other 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.

CSIS policy and procedures

CSIS governance of the TRM program[22]

[17] CSIS Memo, "Progress of TRA Operationalization," File May 5, 2015.
[18] *CSIS Act,* subsection 12.1(1)
[19] *CSIS Act*, subsection 12.1(2).
[20] *CSIS Act*, subsections 12.1 (3.1), (3.2) and (3.4).
[21] *CSIS Act,* subsections 12.1(2) and (3).
[22] Governing Policy: Conduct of Operations, S.12.1 Threat Reduction Measures.
[23] Conduct of Operations, section 12.1 Threat Reduction Measures, and CSIS Briefing by TRM to NSIRA on July 9, 2020.
[24] Conduct of Operations, section 12.1 Threat Reduction Measures,
[25] Conduct of Operations, section 12.1 Threat Reduction Measures,
[26] Conduct of Operations, section 12.1 Threat Reduction Measures,
[27] Conduct of Operations, section 12.1 Threat Reduction Measures,
[28] NSIRA noted that in addition to the overarching TRM policy and procedures, the TRM policy suite also

28. CSIS policy distinguishes types of TRM approvals:

Description of the legal standards

29. CSIS may only undertake a TRM under subsection 12.1(1) of the *CSIS Act* "if there are reasonable grounds to believe" certain conduct is a threat to the security of Canada.[31] This requirement of "reasonable grounds to believe" is a higher standard than the "reasonable grounds to suspect" threshold CSIS must meet to exercise its intelligence collection powers under section 12 of the *CSIS Act*.[32]

30. Unlike reasonable grounds to suspect, which connotes a mere possibility, the reasonable grounds to believe standard is based on an assessment of probability.[33]

Interpretation of the legal standards

31. Under subsection 12.1(2) of the *CSIS Act*, before implementing a TRM, CSIS must consider the nature of the threat, the nature of the measures, and the reasonable availability of other means to reduce the threat.

It assesses the following in particular:

[29]

[30] CSIS Conduct of Operations S12.1 Threat Reduction Activities
[31] *CSIS Act* ss 12.1(1).
[32] *CSIS Act* s 12(1).
[33] *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 based on information that is relevant, current, accurate, precise, compelling, and reliable.
[34] *CSIS Act*, subsection 12.1(2).
[35] *R v. Oakes*, [1986] 1SCR 103 at paras 69-70.

NSIRA agrees with the

IV FINDINGS AND RECOMMENDATIONS

Compliance and governance of TRMs

33. As part of the compliance sample, NSIRA scrutinized TRMs targeting foreign influence activities carried out by hostile state actors against Canadians and Canadian democratic institutions. The review assessed these measures against legislative and policy requirements, as well as Ministerial Direction.

Compliance with MD and the CSIS Act

37. As noted above, Ministerial Direction confers on CSIS two specific obligations in the context of TRMs: first, CSIS must assess the operational, political, foreign relations and legal risks of the proposed TRM, and second CSIS must consult its government partners.

[36] Request for Approval for
[37] See
[38]

[39] Request for Approval

38. **Finding no. 1: For all of the TRM reviewed, NSIRA finds that CSIS met the requirements set out in Ministerial Direction as articulated in CSIS Policy and Procedures.**

[41] CSIS Glossary in CSIS Governance System (CGS)

NSIRA agrees with the

NSIRA analyzed material related to

NSIRA noted that

45

According to NSIRA's file review

NSIRA sought additional information from CSIS to confirm

52. NSIRA's own legal assessment concludes that where CSIS there was no rational link between the intervention and the reduction of the identified threat. In these cases, because there was no rational link, CSIS's intervention was not reasonable and proportional in the circumstances, as required by subsection 12.1(2) of the *CSIS Act*.

53. **Finding no. 2: NSIRA finds that CSIS conducted in a manner that was not reasonable and proportional as required by section 12.1(2) of the *CSIS Act*.**

Subject selection:

[48] Note that for

[50] CSIS response to NSIRA Subject Selection RFI,
[51] CSIS response to NSRIA Subject Selection RFI,
[52] NSIRA requested for information dated October 6, 2020, October 16, 2020 and October 21, 2020, among others.
[53] CSIS comments on NSIRA's Draft TRM Review, November 30, 2020.

55. **Finding #3: for this TRM, NSIRA finds that they met the requirements of the *CSIS Act*. In this instance, NSIRA finds that CSIS's selection reflected a strong rational link between the threat and the measure.**

Documentation

58.

59.

60. **Finding no. 4: NSIRA finds that CSIS does not have a formalized and documented process to help guide the identification and selection of subjects for inclusion in TRMs that ensures proper accountability for these activities.**

Recommendation no. 1: NSIRA recommends that CSIS create an accountability framework for information related to TRMs, and that this information be documented and retained in a central, easily retrievable location.

[54] NSIRA RFI dated September 15, 2020; NSIRA RFI Subject Selection dated October 6, 2020; and NSIRA Subject Selection RFI 2 dated October 16, 2020.
[55] SIRC Review 2016-09.

[redacted] Recommendation no. 2: NSIRA recommends that CSIS create a formalized and documented process that ensures pertinent facts regarding TRM subjects are provided to NSLAG to ensure that it has the information necessary to provide considered legal advice on the identification and selection of interviewees for inclusion in TRMs.

Other conditions:

The file review revealed that CSIS's operational units, working with CSIS's Intelligence Assessment Branch (IAB),

Finding no. 5: NSIRA finds that the

67. NSIRA observes that

[58] See Annex C for additional details.
[59]

68. **Finding no. 6: NSIRA finds that CSIS**

Recommendation no. 3: NSIRA recommends that CSIS develop an accountability framework for compliance with legal advice on TRMs, including documenting when and why legal advice was not followed.

Effectiveness of TRMs

NSIRA notes that the effectiveness of

72.

60

62 CSIS Briefing to NSIRA on October 2, 2020.
63 CSIS Briefing to NSIRA on October 2, 2020

As part of future considerations of similar TRMs,
NSIRA would expect

Compliance and Governance of TRMs

74. As part of the compliance sample, NSIRA also examined TRMs[64]

The resulting findings and recommendations are discussed below.

NSIRA examined documents related to

Compliance with MD and the CSIS Act

77. As noted earlier, Ministerial Direction confers on CSIS two specific obligations in the context of TRMs: CSIS must assess the operational, political, foreign relations and legal risks of the proposed TRM, and CSIS must consult with its government partners.

78. **Finding no. 7: For all TRMs reviewed, NSIRA finds that the requirements set out in Ministerial Direction were met.**

79. In its assessment of compliance with the *CSIS Act*, NSIRA was again attentive to

64

80. Accordingly, NSIRA expected to see

Detailed criteria

The review examined

82. **inding no. 8: NSIRA finds that the demonstrated a high degree of rigour**.

NSIRA noted, however,

NSIRA's recommendation number one, above, that

The creation of

Subsection 12.1(3.2) of the *CSIS Act* is one of two statutory "triggers" for CSIS to obtain a warrant before carrying out a TRM.

68

Downstream* Charter *obligations

he *CSIS Act* is clear that when a proposed TRM would limit a right or freedom, a warrant must be sought.

88.

89. **Finding no. 9: NSIRA finds that**

Recommendation no. 4: NSIRA recommends that when considering whether a *Charter* right is limited by a proposed TRM, NSLAG should undertake case-by-case legal analysis that assesses

90. NSIRA will reserve judgment on compliance with the *CSIS Act*, until it can fully explore these issues.

Effectiveness of TRMs

91. Of the TRMs that were implemented, CSIS deemed to have been at least partially successful.

VI CONCLUSION

96. The legal issues and questions raised in this review point the way to further reviews by NSIRA. In particular, NSIRA was struck by the potential for leveraging TRMs to affect rights and freedoms protected under the *Charter*, and in future NSIRA will pay particular attention to this class of TRMs and the associated legal risks.

97. In addition, this review has highlighted the importance

of CSIS's threat reduction mandate and the range of the requirements in the *CSIS Act* that each TRM must meet. To perform its function,

NSIRA expects that some TRMs could create between CSIS and third parties.

99. Finally, this review uncovered inconsistencies in CSIS's internal approval process and in the documentation of certain TRMs,

It also renders more difficult for NSIRA the task of reviewing TRMs for compliance. As discussed above, CSIS should address these issues in future.

Annex A: Overview of CSIS Use of TRMs 2015 – 2019

100. This is NSIRA's first review of CSIS's use of its threat reduction powers. To provide a broad perspective on the use of these powers, NSIRA analysed information on all TRMs taken by CSIS since 2015, including not only TRMs that were approved and implemented, but also those that were denied or abandoned. This exercise will assist us in selecting topics for future review.

Types of TRMs

101. There are three broad categories of TRMs implemented by CSIS: messaging, leveraging, and interference.

102. Messaging TRMs to date have involved the following:

103. Leveraging TRMs have involved activities such as:

104. Interference TRMs have included activities such as:

105. By a slight margin, leveraging is the most commonly proposed TRM

106. Over the years, the leveraging category has seen the greatest growth in the number of proposals put forward,

107. NSIRA did not complete an in-depth examination of all three types of TRMs. Based on the summaries provided by CSIS on each class of TRM and on the results of this review; NSIRA will prioritize leveraging TRMs in future reviews, as these appear to carry the highest risk of limiting *Charter*-protected rights and freedoms.

Requests,

108. CSIS has proposed the use of TRM powers times between 2015 and 2019.[86]

NSIRA notes that, over the past five years, TRM activities have been used to target the full spectrum of national security threats as defined in the *CSIS Act*.

In a briefing with CSIS's TRM unit, it was explained

113.

The TRM unit has developed a presentation to be provided in person to operational staff in all CSIS regional offices.

CSIS was able to visit Atlantic Region, Ottawa Region, Toronto Region and Quebec Region. COVID-19 related travel restrictions have limited CSIS's ability to complete the delivery of this presentation to all CSIS regions.

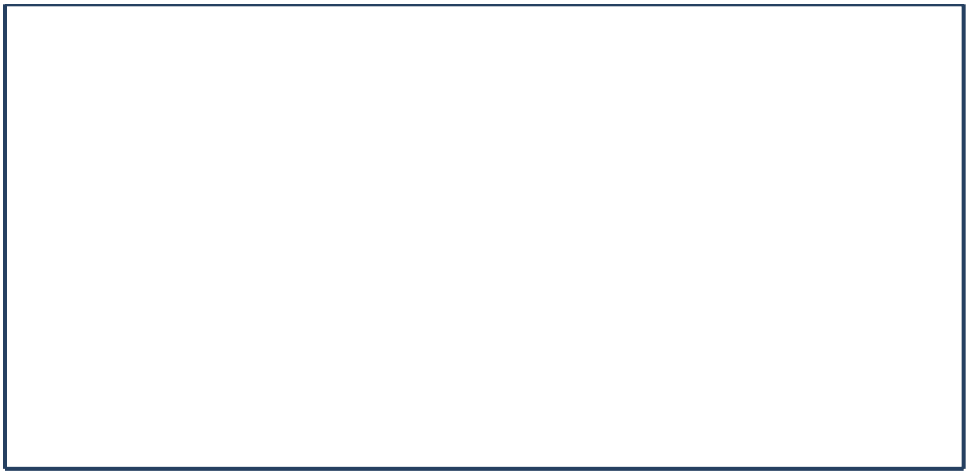
114.

[90] CSIS Briefing by TRM Unit, July 9, 2020.
[91] CSIS Briefing by TRM to NSIRA on July 9, 2020.

Distribution by branch[94]

115. CSIS's Counter-Terrorism Branch (CT) has requested TRMs, representing of all proposed TRMs. Counter-Intelligence / Counter-Proliferation Branch (CICP), have requested a combined TRMs, representing of all proposed TRMs – respectively.

This divergence peaks in 2017 when



117.

As of September 2019, CSIS reports having CT targets and CICP targets.[96] As noted above, in 2019, each branch only

[92] TRM fo 2020 11 06 and CSIS Briefing by TRM to NSIRA on July 9, 2020.
[93] Email correspondence dated June 4, 2019 re Dir Request – briefing on warranted TRMs and C-59.
[94] During the period under review,

[96] *Dedicated to National Security, CSIS Transition Material for the Minister of Public Safety and Emergency Preparedness,* November 2019.

119. Overall, since 2015, while CSIS's use of TRM powers remains limited, CSIS has been applying TRM powers to the full spectrum of national security threats mandated under the *CSIS Act*.[97]

[97] CSIS is mandated to investigate threats to the security of Canada as defined in s. 2 of the *CSIS Act,* specifically espionage or sabotage, foreign influenced activities, terrorism and subversion.

Annex B: Scope and Methodology

120. The review encompassed all threat reduction activities since 2015, with a focus on the period of November 2018 to December 2019 for the compliance sample.[98] NSIRA also examined some documentation that fell outside this period in order to obtain a complete picture of relevant issues.

121. In preparing this review, NSIRA examined corporate, operational and legal documents, previous reviews, pertinent Government of Canada legislation, academic journals, and relevant court decisions.

122. In order to identify a specific aspect of CSIS's activities on which to focus, NSIRA undertook a survey of all CSIS TRMs[99] and attended a preliminary briefing with CSIS's [100]

123. NSIRA chose to focus its compliance exercise on CSIS's threat reduction activities associated with foreign influence and threats to Canadian democratic institutions. This decision was made in part because of the timeliness and relevance of the topic, and in part because the range of actions taken in relation to this threat in 2019 made for a rich but manageable sample.

124. NSIRA researchers presented their review plan to the NSIRA member champion for approval and provided CSIS with a Terms of Reference in September 2020.[101]

125. NSIRA scrutinized electronic records, files, correspondence and other documentation associated with the sample of TRM cases to assess compliance with the *CSIS Act,* Ministerial Direction and applicable CSIS policies and procedures. NSIRA also assessed whether the TRMs were compliant with other Canadian laws, including the *Charter*. The document review was supplemented with briefings from relevant CSIS stakeholders to gain additional information and a contextualized understanding of the activities.[102]

126. NSIRA used several lines of evidence to support the review's findings. Researchers examined all documents provided by CSIS, but also sought, retrieved and reviewed documents directly from CSIS's databases.

127. While NSIRA is entitled to unfettered access to CSIS information under the *NSIRA Act*, restrictions in place due to COVID-19 meant that for much of the period of this review, NSIRA faced limited access to CSIS facilities, from where most review of CSIS is normally conducted. In order to compensate for the situation, CSIS offered to undertake some of the required research in support of this review – research that NSIRA staff would normally undertake themselves. This additional burden was taken on despite CSIS's own resource constraints stemming from the COVID-19 situation.

---

[98] Ministerial Direction for Operations and Accountability, 2015, Appendix 1 – Risk, and Ministerial Direction for Accountability, 2019, Annex A – Risk Assessment. The last TRM review completed by SIRC was published in January 2019, and reviewed activities between November 1, 2017 and November 1, 2018. See SIRC Review 2018-06.
[99] Information used in the development of the TRM database was provided by CSIS in response to NSIRA requests dated June 15, 2020 and July 20, 2020.
[100] CSIS briefing by TRM Unit to NSIRA on July 9, 2020.
[101] NSIRA Terms of Reference: Review of CSIS Threat Reduction Measures, dated September 11, 2020.
[102] CSIS briefing by CICP, TR, and TRM Unit to NSIRA on October 2, 2020.

Annex C: Findings and Recommendations

Findings

1. For all of TRMs reviewed, NSIRA finds that CSIS met the requirements set out in Ministerial Direction as articulated in CSIS Policy and Procedures.

2. NSIRA finds that CSIS conducted in a manner that was not reasonable and proportional as required by section 12.1(2) of the *CSIS Act*.

3. Of the for this TRM, NSIRA finds that they met the requirements of the *CSIS Act*. In this instance, NSIRA finds that CSIS's selection reflected a strong rational link between the threat and the measure.

4. NSIRA finds that CSIS does not have a formalized and documented process to help guide the identification and selection of subjects for inclusion in TRMs that ensures proper accountability for these activities.

NSIRA finds that

NSIRA finds that CSIS

7. For TRMs reviewed, NSIRA finds that the requirements set out in Ministerial Direction were met.

8. NSIRA finds that the
demonstrated a high degree of rigour

9. **NSIRA finds that**

Recommendations

1. NSIRA recommends that CSIS create an accountability framework for information related to TRMs, and that this information be documented and retained in a central easily retrievable location.

NSIRA recommends that CSIS create a formalized and documented process that ensures pertinent facts regarding TRM subjects are provided to NSLAG to ensure that is has the information necessary to provide considered legal advice on the identification and selection of interviewees for inclusion in TRMs.

3. NSIRA recommends that CSIS develop and accountability framework for compliance with legal advice on TRMs. Including documenting when and why legal advice was not followed.

4. NSIRA recommends that, when considering whether a *Charter* right is limited by a proposed TRM, NSLAG should undertake a case-by-case legal analysis that assesses