THE CSIS-RCMP RELATIONSHIP IN
THROUGH THE LENS OF AN ONGOING INVESTIGATION

(NSIRA REVIEW 2019-04)

I EXECUTIVE SUMMARY

1. The relationship between CSIS and the RCMP is central to Canada's national security architecture. CSIS has a broad mandate to collect intelligence and advise government on threats to national security, but it is not a police service. The RCMP investigates national security criminal activities, and collects evidence in support of prosecution. To effectively counter national security threats, CSIS and the RCMP must work together.

2. In this review, NSIRA examined the state of the relationship between CSIS and the RCMP through the lens of an ongoing investigation NSIRA undertook an in-depth study of both agencies' operations, with particular attention to how the two agencies collaborated on this investigation in recent years, both and at headquarters. Although the findings of this review are specific to the investigation, NSIRA has no reason to believe that the investigation in question is atypical, and thus this review provides insight into the more general state of the two agencies' relationship.

3

NSIRA also observed how issues of candour with the Federal Court, and the Federal Court's discovery of longstanding legal problems with CSIS human source activities, have affected CSIS operations. Indeed, the repercussions of CSIS's conduct have sharply limited its ability to collect intelligence on the threat in question, resulting in gaps. NSIRA recommends that CSIS invest the resources needed to develop alternate sources of collection in order to minimize the risk of further damage to the investigation.

4. NSIRA found that the agencies have developed a strong relationship that has fostered effective tactical de-confliction of operational activities. Nonetheless, technological constraints are making CSIS-RCMP de-confliction excessively burdensome and time-consuming. NSIRA recommends that CSIS and the RCMP prioritize the deployment of usable and compatible secure communications systems in order to make regional de-confliction more efficient.

5. The RCMP's use of CSIS information in support of criminal prosecutions has long been limited by what are seen as the risks of involving CSIS or CSIS information in a prosecution. The resulting disclosure requirements are seen as putting CSIS sources and methods at risk of exposure; the overriding need to protect those sources and methods complicates, and can even jeopardize, potential prosecutions. Termed the "intelligence-to-evidence" problem, this shared understanding guides the actions of both CSIS and the RCMP. Indeed, NSIRA observed a general reluctance on the part of both agencies to connect CSIS information to an RCMP investigation.

6. The current framework guiding the CSIS-RCMP relationship is "One Vision 2.0", which sets out principles and guidelines to manage the risks of interaction and information sharing between the two agencies. One Vision 2.0 has left fundamental issues related to the intelligence-to-evidence problem unresolved, however. In the case of the investigation in question, despite frequent verbal exchanges between CSIS and RCMP headquarters, CSIS's formal disclosures of information have been very limited and not always useful. CSIS intelligence has not been shared or used in a way that has significantly advanced the RCMP's investigations.

7. On the whole, NSIRA found that CSIS and the RCMP have made little progress in addressing the threat under investigation. Moreover, CSIS and the RCMP do not have a shared vision or joint long-term strategy to address the threat. NSIRA recommends that the two agencies develop a properly resourced joint strategy to address the criminal activities related to the threat. This strategy should consider the full range of tools available to both agencies.

8. An external review of CSIS and the RCMP's operational relationship was completed in 2019. Called the Operational Improvement Review, it set out ambitious recommendations to improve the way in which CSIS and the RCMP jointly manage threats while managing the risks of CSIS disclosure to the RCMP. The Operational Improvement Review has the support of senior management in both organizations, and work is underway to assess and implement its recommendations. NSIRA recommends that both agencies continue to prioritize the timely implementation of the Operational Improvement Review. At the appropriate time in the coming years, NSIRA will launch a review of CSIS and the RCMP's implementation of the Operational Improvement Review in order to assess progress and take stock of the results.

II AUTHORITIES

9. This review was conducted pursuant to paragraphs 8(1)(a) and 8(1)(b) of the *National Security and Intelligence Review Agency Act*.

III INTRODUCTION

10. The relationship between CSIS and the RCMP is central to Canada's national security architecture. CSIS has broad investigative powers regarding threats to the security of Canada and a mandate to advise government, but it is not a police force. The RCMP has a mandate to investigate national security criminal activities, and collects evidence to be used in prosecuting these criminal activities. To effectively counter national security threats, CSIS and the RCMP must work together.

11. The predecessor to NSIRA, the Security Intelligence Review Committee (SIRC), could only review bilateral or multilateral relationships from CSIS's perspective. By contrast, NSIRA's interdepartmental review mandate gives it the ability to review both the CSIS and RCMP sides of national security investigations.

12. For this review, NSIRA focussed on the CSIS-RCMP relationship by undertaking an in-depth study of an ongoing investigation in which they are both involved.

13. Specifically, NSIRA selected the ongoing investigation of Canada-based extremists

14. This is amongst the first inter-agency reviews that NSIRA has carried out under its new mandate

IV ANALYSIS

CSIS

20. The CSIS investigation into began in

:he investigation has waxed and waned, but CSIS has generally assessed the risk of a large-scale attack

21. In 2015, CSIS noted an increase in threat-related activity by

22. In investigating CSIS's primary domestic partner is the RCMP. CSIS and the RCMP engage frequently using the bilateral "One Vision 2.0" framework to guide and structure information sharing and the de-confliction of their respective investigations. This framework, and its limitations, is discussed in detail below. Other domestic partners include the CBSA, CRA and FINTRAC. CSIS also shares intelligence with international partners

Challenges with the Federal Court

33.

CSIS, as a matter of routine, many of whom are valuable precisely because of their involvement in, or exposure to, terrorist activity. Under the *Criminal Code*, however, support for terrorist activity is unlawful. CSIS had for many years maintained that it was shielded from criminal liability for actions such as these by the legal doctrine of Crown immunity. Despite this, the applicability of Crown immunity to CSIS had been called into

34. n February 2018, in the course of reviewing the legal risks associated with CSIS's human source activities, CSIS's Departmental Legal Services Unit (DLSU), which forms part of the National Security Litigation and Advisory Group (NSLAG) within

[42] SIRC's review of foreign fighters was undertaken in 2015 and completed in 2016. SIRC, *CSIS's investigation of 'foreign fighters'*, May 27, 2016.

the Department of Justice

35. In April 2018, while hearing an application for CSIS warrants, the Federal Court

that CSIS had used information derived from seemingly illegal activities in support of several warrant applications.

At no point had CSIS volunteered to the Court that there were questions regarding the legality of some of its

36.

CSIS's Deputy Director of Operations (DDO) issued a directive stating that no new operations assessed as "high legal risk" (i.e., very likely unlawful) would be approved, and requiring that all such ongoing operations be reviewed and modified so as to reduce their level of legal risk.[49]

Impact

37.

submitted a new operational plan in accordance with the new DDO directive.[50]

n response, proposed a second alternative operational plan, which was ultimately approved

[48] Senior General Counsel to CSIS Director,

[49] CSIS-DDO, *Interim Direction on the Conduct of Operations Likely Involving the Commission of Criminal Offenses*, January 17. 2019.

Impact on CSIS warranted collection

39. Given the legal problems associated with

DDO ordered that information previously collected be isolated from CSIS's operational database.[54] This meant that all of the warranted material collected, and all subsequent reports generated on the basis of that information, were no longer useable or accessible.

40. As the Court's enquiries into CSIS's seemingly unlawful activities stretched on, the Court decided to permit a return to normalcy in order to minimize the risks to national security.

CSIS's candour to the Federal Court

41. It was in this fraught legal context that the concerns regarding emerged Not only did these allegations pose a challenge for CSIS's management of but they also raised broader questions

42. response to these allegations, CSIS in order to take stock of the full range of concerns

44. during the course of CSIS's internal review was becoming apparent that CSIS had not been forthcoming with the Court

Effect on the investigation

46. At this point, CSIS's investigation reached its nadir.

47. Following the Royal assent of Bill C-59 on June 21, 2019, CSIS obtained a new statutory justification framework for human source activities designed to address the legal issues that had arisen [65] Under this regime, CSIS and its human sources would be able to resume the full range of collection activities. First, though, the new legislative provisions required the Minister of Public Safety and Emergency Preparedness to determine the classes of otherwise unlawful acts or omissions that CSIS employees would be justified in committing, or in directing another person (such as a human source), to commit. Then, the newly-formed Intelligence Commissioner had to review the Minister's determination.

[63] CSIS's answers to NSIRA questions, [email], October 21, 2020

[65] *National Security Act* (2017); CSIS, *OPS-1200: Section 20.1 Justification Framework*, July 15, 2019.

Current status of the investigation

Resourcing and other investigative challenges

51. In conversation with both and CSIS headquarters, NSIRA asked why it was that CSIS's investigation
NSIRA was informed that

52. In conversations with front-line investigators, NSIRA was informed that resource limitations have constrained the scope of the investigation.

[81] Briefings from December 9-12, 2019.
[82] Briefings from December 9-12, 2019.
[83] Briefings from December 9-12, 2019.

54. CSIS is aware of the vulnerability of its investigatior

55. **Finding no. 1: Since 2019, there have been significant gaps in CSIS's intelligence collection on the threat posed by**

56. **Finding no. 2: Reliance on makes CSIS's investigation into**

Recommendation no. 1: NSIRA recommends that CSIS invest the resources needed to avoid having to

The RCMP

57. Among the RCMP's mandates, the organization is charged with investigating and preventing national security criminal activities in order to ensure public safety.[87] Within the RCMP's Federal Policing program, national security criminal investigations are overseen and coordinated by the Federal Policing National Security (FPNS) unit at RCMP headquarters in Ottawa. The goal of FPNS is to provide centralized management of national security criminal investigations in order to ensure that they comply with legislation, Ministerial Direction and internal policy.[88]

58. FPNS is not an investigative unit; rather, national security criminal investigations are carried out by teams in the RCMP's regional divisions. Those divisions with more resources dedicated to national security have Integrated National Security Enforcement Teams (INSETs), while those with fewer resources have National Security Enforcement Sections (NSESs). Some divisions have neither, but are covered by units in neighbouring divisions.[89] The RCMP division responsible for conducts national security criminal investigations.

59. FPNS is responsible for all exchanges of national security information with foreign entities as well as with federal non-law enforcement departments and agencies, such as CSIS

[87] *Security Offences Act*, section 6(1). The RCMP's authority to investigate national security-related offences is derived from several additional acts, including the *Royal Canadian Mounted Police Act* (s. 18), the *CSIS Act,* the *Security of Information Act* and the *Criminal Code*.
[88] Centralized control stems from the 2003 Ministerial Direction that "All investigations… [relating to national security] be centrally coordinated" to enhance operational accountability: quoted in RCMP, "Governance Framework: National Security Criminal Investigations," January 8, 2018, page 9.
[89] RCMP, "Governance Framework: National Security Criminal Investigations," January 8, 2018, page 9.

and FINTRAC. The INSETs and NSESs are responsible for exchanges with domestic law enforcement.[90] With regard to all information exchanged with CSIS is handled by International partners include police services

60. The RCMP has been investigating in Canada . When NSIRA visitec in the fall of 2019, had three national security criminal investigations related to

61.

CSIS-RCMP Coordination and Information Sharing

62. nformation sharing between intelligence and police services is critical to mounting a coordinated and effective response to national security threats.[97] Despite this, CSIS and the RCMP's different mandates and ways of operating, along with the experience of several high-profile cases over the past several decades, have reinforced a shared aversion to the exchange of information between the organizations. CSIS is reluctant to formally disclose information to the RCMP for fear that its sensitive sources and methods could be placed in jeopardy in the event that the shared information is involved in a future prosecution or other judicial proceeding. The RCMP's reluctance to include CSIS information in its investigative records stems from a similar fear, namely, that CSIS's involvement in a criminal investigation could complicate or even jeopardize the prosecution of alleged criminals. These challenges have been termed the "intelligence-to-evidence" problem, which dates back to the creation of CSIS as an entity apart from the RCMP in 1984.

63. Starting in the 1980s, a number of Memoranda of Understanding between CSIS and the RCMP were developed to encourage information sharing, while ensuring the separation of investigations.[98] Particularly after September 11, 2011, CSIS and the RCMP recognized that,

---

[90] Criminal Operations (CrOps) Officers are responsible for exchanges with domestic non-law enforcement agencies (provincial/territorial, municipal and non-governmental).

[91] is the RCMP's partner, and provides a significant amount of information related to n Canada.

[92]

[93]

[94]

[95]

[96]

Operational Improvement Review, March 2019, page 55.

[98] Memoranda of Understanding between CSIS and the RCMP were struck in 1984, 1986, and one in 1989. The evolution of CSIS and the RCMP's MOUs is detailed in

despite the constraints imposed by the intelligence-to-evidence dilemma, their tendency not to engage with each other was hindering effectiveness, and that they needed to find better ways to work together to protect public safety. also stressed the need for improved collaboration. In 2012, the two agencies jointly launched the One Vision framework. The framework did not purport to solve the intelligence-to-evidence issue, but rather sought to ensure that the CSIS and the RCMP could share information and remain broadly aware of each other's activities in order to effectively address threats to public safety, while at the same time managing the relationship in such a way as to minimize the potential for unintended problems to arise.

64. The One Vision framework was amended in late 2015 to become One Vision 2.0.[100] One Vision 2.0 further formalized information sharing and collaboration between CSIS and the RCMP, in part to prevent CSIS and RCMP investigations from becoming too closely linked, and in part so that information sharing between the two agencies could be explained and defended before the courts.[101]

The One Vision 2.0 framework

65. One Vision 2.0 sets out several different types of meetings by which CSIS and the RCMP can discuss and manage threats to national security and criminal activity. These include "Strategic Case Management" meetings between CSIS and the RCMP headquarters, of which there are two variants: two-pillar meetings, involving only CSIS and RCMP headquarters, and four-pillar meetings, involving headquarters as well as the relevant CSIS region and RCMP division.[102]

66. For the nvestigation, CSIS and the RCMP use Strategic Case Management meetings to advise one another of information obtained from partner agencies and to provide high-level updates on investigations, and to ensure that the actions taken by one agency do not influence the other's investigations or overall strategy. These meetings are also used to determine which agency will lead investigative efforts into specific threats or individuals. This concept, known as "primacy", although not formally part of the One Vision 2.0 framework, reflects a general desire to minimize the extent to which the two organizations each run full investigations of the same issue in parallel. Although parallel investigations continue to exist, NSIRA heard that they are considered less than ideal because of their inefficiency and because of the risk that the two investigations will become intertwined, thereby putting CSIS information at risk of disclosure in a prosecution; having a single clear lead helps to manage this risk.[103]

In 1999 *National Security Offences Review* of the RCMP's program noted that *Regina vs. Stinchcombe* had further restricted CSIS and the RCMP's ability to exchange information.

[100] *CSIS-RCMP Framework for Cooperation: One Vision 2.0*, November 10, 2015. Signed by both parties on November 24, 2015.
[101] CSIS-RCMP, "CSIS and RCMP: One Vision 2.0 – An Operational Approach to Intelligence and Evidence," [PowerPoint deck], January 26-27, 2016.
[102] *CSIS-RCMP Framework for Cooperation: One Vision 2.0*, November 10, 2015.
[103] Joint briefing from RCMP and CSIS on the Operational Improvement Review, October 10, 2019. One Vision 2.0 provides for parallel but separate investigations, to ensure that CSIS remains a third-party and the RCMP is not required to disclose its information. According to the Supreme Court decision in *R. v. Stinchcombe* (1991), the Crown has an obligation to disclose anything within the "fruits of the investigation". CSIS files become part of this disclosure if the files are in the control of the prosecution -- a situation that may occur if a CSIS and RCMP investigation is so intertwined that they have become

Formal disclosures of information by CSIS to the RCMP and discussions of CSIS threat reduction measures may only occur between headquarters within a two-pillar Strategic Case Management meeting, except in exigent circumstances.[104]

67. One Vision 2.0 also sets out guidelines for tactical de-confliction between CSIS regions and RCMP divisions at the "field level" without the involvement of headquarters. Tactical de-confliction is intended to prevent overlap between the two agencies' operational activities thereby giving CSIS the opportunity to flag potential issues, with the goal of helping ensure that its planned actions do not conflict with ongoing CSIS investigations and that CSIS and RCMP investigations remain separate. For its part, CSIS will sometimes advise the RCMP of The two agencies also frequently consult each other to ensure that they do not cross paths during [105]

68. Under One Vision 2.0, CSIS disclosures of information to the RCMP may take one of two forms: (1) advisory letters, which contain information that the RCMP can use as evidence to obtain warrants or can otherwise use in Court; and (2) disclosure letters, which contain information that the RCMP can use as an investigative lead or 'tip', so that investigators may then collect their own evidence; disclosure letters should not end up in legal proceedings.[106]

69. Disclosure and advisory letters do not represent the full extent of the information exchanged between CSIS and the RCMP, however. During One Vision 2.0 exchanges, CSIS and the RCMP will discuss their respective investigations to the extent needed to de-conflict. These discussions, and the resulting records of decision, can be quite detailed, with the organizations listing the individuals they are investigating, or speaking frankly about gaps or other factors that might (for instance) make one organization the right choice to take the investigative lead for a certain individual or issue.[107]

70. In order to avoid having CSIS information leak into RCMP investigations, however, the RCMP participants in One Vision 2.0 discussions are limited to individuals from FPNS and/or senior officers from the divisions (typically at the Inspector level or above), depending on the type of meeting. For Strategic Case Management meetings, records of decision are drafted by CSIS and then sent to RCMP headquarters, which often chooses not to pass them to the divisions.

71. The RCMP officers directly involved in national security criminal investigations, whose decision-making rationales and records are subject to disclosure during a prosecution, are by these means deliberately excluded from conversations with CSIS or exposure to CSIS information. In this way, the RCMP protects CSIS information by preventing it from entering the records or influencing the decision-making of front-line RCMP investigators, where it could end up being subject to disclosure during a prosecution.[108]

---

one investigation." Department of Justice, "General Legal Principles Regarding Intelligence and Evidence," [deck], September, 2012.

[104] It is understood that if, for example, there were a threat to an RCMP officer, the CSIS region could quickly inform the INSET rather than go through Headquarters to make this kind of disclosure. CSIS-ADC, *Direction to the regions on information sharing with the Royal Canadian Mounted Police – One Vision 2.0*, July 16, 2016.

[105] NSIRA's review of One Vision 2.0 Records of Decision, 2016-2020.

[106] *CSIS-RCMP Framework for Cooperation: One Vision 2.0*, November 10, 2015, page 2.

[107] NSIRA's review of One Vision 2.0 Records of Decision, 2016-2020.

[108] Joint briefing from RCMP and CSIS on the Operational Improvement Review, October 10, 2019.

The CSIS-RCMP relationship

72. In discussion with CSIS and RCMP employees, NSIRA heard that in recent years, and particularly since the advent of One Vision 2.0, the level of frank discussion between CSIS and RCMP headquarters has greatly improved. NSIRA was also informed that the relationship between had improved significantly, particularly over the last two years.[109] Senior management in both organizations has prioritized the building of strong ties, and the number of tactical de-confliction meetings has increased.

73. NSIRA also heard, however, that the improvement was largely the result of individual relationships, and that there remain serious gaps and challenges that continue to limit information sharing and the overall effectiveness of the two agencies' collaboration in national security matters. Indeed, echoed one another when they told NSIRA that they make the relationship work despite the serious limitations of the One Vision 2.0 framework.[110]

74. Over the course of this review, NSIRA examined over sixty One Vision 2.0 records of decision from between 2016 and 2020 related to This included records for two-pillar and four-pillar Strategic Case Management meetings, as well as tactical de-confliction between NSIRA also examined all disclosures of CSIS information to the RCMP within the context of the investigation.[111]

75. Between 2016 and 2020 CSIS provided the RCMP with zero advisory letters and six disclosure letters related to the investigation. Of these, two disclosure letters sought to help the RCMP initiate a criminal investigation into an individual, while the other four sought to make the RCMP

76. This same pattern of relatively few advisory letters but more disclosure letters within the investigation is reflected when one looks CSIS-wide. Across all of its investigations, CSIS produced zero advisory letters and 35 disclosure letters in 2016; three advisory and forty-eight disclosure letters in 2017; four advisory and 31 disclosure letters in 2018; and eight advisory and 27 disclosure letters in 2019.[113]

77. In reviewing specific instances where CSIS and the RCMP discussed the possible formal disclosure of information to the RCMP, NSIRA noted a general pattern of reluctance. On several occasions, the RCMP could have received important information to advance its investigation from CSIS, but instead sought disclosure from a police partner, even though doing so delayed the RCMP's investigation. In one example, after learning from CSIS of the RCMP

[109] Briefings from December, 9-12, 2019; Briefings from December 10, 2019.
[110] Briefings from December, 9-12, 2019; Briefings from December 10, 2019.

[113] Operational Improvement Review, March, 2019, page 55; CSIS statistics provided to NSIRA, [email], November 12, 2020.

spent eight months attempting unsuccessfully to get information from to use as grounds to proceed with an investigation.[114]

78. NSIRA was struck by the roundabout ways in which CSIS tried to provide tactical assistance to the RCMP without making formal disclosures of information.

79. These instances illustrate a mutual reluctance to pursue the formal disclosure of information from CSIS, even in cases where the alleged threats were serious or imminent, and even though the alternative investigative path was slower and involved different challenges.

Results of disclosure

80. In cases where CSIS did disclose information to the RCMP related to the results were mixed. Disclosure letters from CSIS are designed to help orient RCMP investigations by providing the RCMP with a lead or 'tip' to facilitate the RCMP's own collection of evidence.[116]

81. NSIRA was informed by senior officers that many CSIS disclosure letters were "useless".[117] Not only must the RCMP overcome the tensions and contradictions noted above, but the information the letters contain is often deliberately sparse and without context. The contents of disclosure letters are negotiated in advance between CSIS and RCMP headquarters with the goal of minimizing the link back to CSIS. According to FPNS often lacks the necessary granular understanding of the RCMP's investigations to know what information would be useful to

82. In fairness, it should be noted that NSIRA saw instances where the RCMP did take action in response to disclosure letters By contrast, the two letters that pertained to did not appear to advance the RCMP's investigation.[119]

---

[115] Briefings from December 9-12, 2019.
[116] Information in CSIS disclosure letters is not to be used as evidence by the RCMP without prior consultation with CSIS. *CSIS-RCMP Framework for Cooperation: One Vision 2.0*, November 10, 2015, page 2.
[117] Briefings from December 10, 2019

Information flow between FPNS and

83. NSIRA also noted issues with respect to the flow of information between RCMP headquarters and In particular, the s often not aware of One Vision 2.0 exchanges between CSIS and RCMP headquarters. After CSIS and RCMP headquarters complete a two-pillar Strategic Case Management meeting, the CSIS regional offices have access to the resulting record of decision. By contrast, RCMP headquarters, represented by FPNS, usually does not provide such records to the relevant divisions. Indeed, NSIRA heard of instances where was not even aware that meetings had taken place with CSIS, even though the meetings pertained to an investigation involving [20] As noted above, even when CSIS information does flow from FPNS to the divisions, it is usually kept at the senior officer level – at least in written form – to prevent it from being recorded by the front-line investigators, where it could end up being subject to disclosure during a prosecution.[121]

84. In speaking with members of NSIRA learned of their frustration with the current FPNS governance model, which leaves the INSET with only the information that FPNS chooses to share. members felt that their exclusion from strategic CSIS-RCMP discussions reduced the usefulness of the exchanges, since FPNS is often unaware of needs and concerns and is thus unable to obtain the necessary assistance from CSIS. According to this limits its ability to advance investigations.[122] Additionally, FPNS is not always aware of resourcing and its constraints, and will sometimes promise support in a two-pillar meeting that is unable to provide. The resulting internal tensions have harmed morale.[123]

85. In the context of the nvestigation, the combined result of the One Vision 2.0 framework and of the FPNS governance model is that CSIS is best informed regarding the overall investigation, followed by FPNS, followed by senior officers while the RCMP investigators actually investigating individuals suspected of criminal activity know the least, and deliberately so. Typically, they have only the fruits of their own investigations.

Case study:

[120] Briefings from December 10, 2019; Briefings from December 9-12, 2019.
[121] Joint briefing from RCMP and CSIS on the Operational Improvement Review, October 10, 2019.
[122] Briefings from December 10, 2019.
[123] Operational Improvement Review, section 2.2.3.1.3(39), March 2019, page 57.

[125] One Vision 2.0 Two-pillar RoD, March 28, 2018; One Vision 2.0 Four-pillar RoD, April 4, 2018.
[126] One Vision 2.0 Two-pillar RoD, April 12, 2018.

87. The most striking aspect was lack of involvement in the decision-making process. All of the discussions and decisions leading up to and decisions took place via two-pillar Strategic Case Management meetings without the involvement of [130] When was told by FPNS to it had limited understanding of what was happening or why. was even unsure as to although FPNS promised that this information would follow.

88. FPNS requested that CSIS give the RCMP a written record of by preparing a disclosure letter that summarized an earlier One Vision 2.0 record of decision.[131] CSIS declined to produce a disclosure letter because, in its view, no formal disclosure had been made, and because it would create unnecessary links [132] As a result, the RCMP did not receive the written disclosure letter that it had requested from CSIS

89. NSIRA reviewers heard from members involved that some of them felt personally exposed for having at FPNS's request without written grounds in hand to justify their actions, although others were of the view that the necessary threshold had been met. Regardless, the events damaged morale at and exacerbated tensions with FPNS.[134] Communication between and FPNS was sufficiently poor that nearly three weeks after members had to ask FPNS whether had had any impact.[135] When NSIRA visited in December 2019, the situation was still vividly recalled.

90. RCMP members also expressed the view that the RCMP risked forfeiting the possibility later on, both because and because, during any future the RCMP would likely have to explain [136]

91. illustrates the problems that can be caused by the RCMP's implementation of the One Vision 2.0 framework, particularly when decisions are made by FPNS with little or no involvement of the INSET.

---

[127] One Vision 2.0 Two-pillar RoD, April 11, 2018 and April 12, 2018.
[128]

[129] pursuant to section 487.11 of the *Criminal Code*. , "Weekly Investigation Report" for , June 22, 2018.
[130] There were four One Vision 2.0 Two-pillar meetings March 29, April 11, April 11 (second Two-pillar meeting and April 12, 2018. and were involved in one Four-pillar One Vision 2.0 meeting, on April 4, 2018, but the decision to act was not made at that meeting.
[131] One Vision 2.0 Two-pillar RoD, May 3, 2018

[133] Briefings from , December 10, 2019.
[134] Briefings from , December 10, 2019.
[135] , "Weekly Investigation Report," April 26, 2018.
[136] Briefings from , December 10, 2019.

Practical barriers to tactical de-confliction between

92. NSIRA heard from both that de-confliction in the region is extremely time-consuming. Given the physical distance between the organizations' buildings and the heavy traffic typical of in-person meetings are inefficient and are impractical as a means of having urgent discussions.[138]

93. **Finding no. 3: A lack of usable and compatible secure communications tools is making CSIS-RCMP de-confliction excessively burdensome and time-consuming.**

Recommendation no. 2: NSIRA recommends that CSIS and the RCMP prioritize the deployment of usable and compatible secure communications systems in order to make regional de-confliction more efficient.

The INSET model

94.

A full evaluation of the INSET model, its strengths and weaknesses, was beyond the scope of this review. NSIRA intends to conduct a dedicated review of the INSET model in future years.

[137] Briefings fron December 9-12, 2019; Briefings from December 10, 2019.
[138] Briefings fron December 9-12, 2019; Briefings from December 10, 2019.
[139] Briefings fron December 9-12, 2019; NSIRA's review of One Vision Records of Decision, 2016-2020.
[140]
[141]
[142]
[143]
[144]

Stalled criminal investigations

95. As will be discussed later in this review, investigations into have struggled to make headway, to the point where in mid-2020 the RCMP was de-prioritizing the investigations and admitted to CSIS that criminal charges remained far off. CSIS, despite the significant problems facing its own investigation has a wealth of reporting Yet little of this information has been provided to the RCMP. Through One Vision 2.0 meetings, RCMP has gained a broad understanding of CSIS's investigation, but the formal disclosures have been of limited use and typically have not reached the actual RCMP investigators. In short, CSIS and the RCMP may de-conflict their activities, but to the advancement of the RCMP's investigations. The investigations remain separate, and intentionally so.

96. This situation is not the result of any breakdown in the personal relationship between key individuals on either side. On the contrary, NSIRA was repeatedly informed by both CSIS and the RCMP that the relationship at present is strong. Nor could one simply portray a risk-averse CSIS as stonewalling the RCMP's demands for information; often it was the RCMP that decided not to request information from CSIS. Ultimately, CSIS and the RCMP appear to be trapped by the constraints that both organizations believe they must operate within in order to avoid compromising prosecutions. CSIS fears the long-term results of disclosure, just as the RCMP often believes that CSIS information 'taints' its investigations.

97. The One Vision 2.0 framework was an attempt to manage these intelligence-to-evidence issues, not overcome them. As such, if the RCMP's investigations are progressing slowly while CSIS – despite the challenges facing its own investigation – continues to amass a trove of intelligence, it is not because CSIS and the RCMP are failing to abide by the letter or spirit of the One Vision 2.0 framework. Rather, it is the result of the overarching conceptual paradigm guiding CSIS and RCMP collaboration.

98. NSIRA heard from employees of both CSIS and the RCMP that are frustrated by this situation; they appreciate all too well how this state of affairs hampers progress in addressing national security issues. CSIS employees expressed exasperation at seeing the RCMP take investigative steps that CSIS knew to be misdirected. RCMP investigators, for their part, were well aware that CSIS (and sometimes also FPNS) had information that could be of use to them, but could not or would not provide it to them; the investigators simply had to carry on as best they could. In the case of

The Operational Improvement Review

99. Both CSIS and the RCMP have acknowledged the shortcomings of the One Vision 2.0 framework, and of the underlying assumptions that the framework reflects. Starting in 2018, the two agencies undertook a joint Operational Improvement Review (OIR) to delve into the intelligence-to-evidence problem and look for ways to address impasses and improve the way in which CSIS and the RCMP work together.[145] The OIR was led by an independent facilitator and lawyer, , who conducted interviews across the country before delivering his final report in March 2019. The report attempts to break down what it presents as the myths and unnecessary barriers impeding effective de-confliction and collaboration between CSIS and the

[145] Joint briefing from RCMP and CSIS on the Operational Improvement Review, October 10, 2019.

RCMP. It makes 76 recommendations to improve the joint management of threats by CSIS and the RCMP.[146]

100. The OIR encourages CSIS and the RCMP to jointly manage threats by using the full range of tools at their disposal. This includes prosecution, but only when it represents the best option.[147] The OIR rejects what it sees as a range of commonly held myths that have constrained cooperation between CSIS and the RCMP, including and in particular the notion that the disclosure of CSIS information to the RCMP automatically 'taints' a police investigation, puts CSIS sources and methods at risk, and must therefore be avoided at all costs.[148] Indeed, during this review, NSIRA saw that exact assumption reflected in the actions of both CSIS and the RCMP throughout the investigation.

101. The OIR encourages the two organizations to abandon these misperceptions and instead to aggressively use the full range of legal tools at their disposal to manage disclosure risks while ensuring that CSIS intelligence can be used more extensively and more effectively by the RCMP. Specifically, the OIR recommends expanding the role of the Public Prosecution Service of Canada (PPSC) in order to bring its expertise to bear in strategic decision-making regarding disclosure, and the management of the attendant risks, from the outset.[149] The OIR also recommends that Strategic Case Management meetings more often include the INSETs, and that records of decision from four-pillar meetings be circulated to all participants.[150] Certainly in this review, NSIRA saw how problems could result from the withholding of information by FPNS from the INSETs. Finally, the OIR recommended that the Government consider certain specific legislative amendments to help protect sensitive information from disclosure.

102. NSIRA heard from CSIS and the RCMP, both and at headquarters, that the OIR was a broadly accurate description of the lived reality of the relationship. NSIRA was also informed that the effort to assess and implement the OIR's recommendations had the backing of senior management in both agencies.[151] Indeed, over the course of this review, NSIRA was able to observe certain changes in practice that seemed to reflect the spirit of the OIR, including the establishment of new joint working groups and an initial uptick in the involvement of the PPSC.

103. NSIRA is of the opinion that the OIR is a complex, ambitious, and promising effort to address longstanding problems that have hindered Canada's ability to prosecute or otherwise address threats to national security. The implementation of the OIR will no doubt prove challenging; it will require changes to policies and procedures, but also deep changes to the culture and mindset of both CSIS and the RCMP.

104. **Finding no. 4: Despite persistent challenges related to information sharing and governance structures, have developed a strong relationship that has fostered effective tactical de-confliction**

[146] Operational Improvement Review, March 2019.
[147] Operational Improvement Review, March 2019, section 2.1.2.2, page 42
[148] Operational Improvement Review, March 2019, section 2.2.1 and 2.2.2, pages 48-52.
[149] Operational Improvement Review, March 2019; NSIRA's review of One Vision 2.0 Records of Decision related to the investigation in question between 2016 and 2020 noted that the RCMP did not have legal counsel present at any of the One Vision meetings; CSIS counsel attended all but one meeting.
[150] Operational Improvement Review, March 2019, Recommendations 14 and 15, page 80.
[151] Joint briefing from RCMP and CSIS on the Operational Improvement Review, October 10, 2019; Briefings from December 9-12, 2019; Briefings from , December 10, 2019.

105. **Finding no. 5: One Vision 2.0 has left fundamental issues related to the intelligence-to-evidence problem unresolved. In the case of despite frequent verbal exchanges between CSIS and RCMP headquarters, CSIS's formal disclosures of information have been limited and not always useful. CSIS intelligence has not been shared or used in a way that has significantly advanced the RCMP's investigations.**

106. **Finding no. 6: The Operational Improvement Review has the support of senior management of both CSIS and the RCMP and work is underway to assess and implement its recommendations.**

Recommendation no. 3: NSIRA recommends that both CSIS and the RCMP continue to prioritize the timely implementation of recommendations from the Operational Improvement Review (OIR) in order to help address the operational shortcomings reported by the OIR and further illustrated in this review.

The Future of the Investigation

107 As noted earlier in this review, CSIS and the RCMP have been investigating n Canada CSIS has collected extensive intelligence This has been in large part through the efforts of

108. Over the last few years, the RCMP has pursued several avenues of investigation, including efforts to build cases

The RCMP has yet to bring any of these efforts to fruition, however. Indeed, admitted to CSIS in fall 2019 that it was having trouble building its investigations Similarly, in December 2019, NSIRA heard directly from that its investigations were at an early stage and not very robust.[154] As of October 2020, CSIS documents note that continues to maintain an open file on but that its investigations are not presently active due to the lack of progress combined with resource constraints caused by competing priorities.[155] In discussions with CSIS, the RCMP has stated that it no longer believes CSIS, for its part, observed that has been

[154] Briefings from December 10, 2019

unable to make progress despite having had ample time to investigate,

109. Although CSIS is not a law enforcement body, it does have tools at its disposal to manage threats to national security. As early as CSIS officials discussed a series of potential threat reduction measures In CSIS officials again discussed these measures with the RCMP

110. CSIS officials have struggled to have their plans approved and implemented. In total, CSIS developed plans for six threat reduction measures Of these, four were not approved, primarily due to legal concerns, and only one was implemented.

111. As of CSIS officials were developing a proposed strategy for responding to that again involved a package of threat reduction measures. The strategy is currently in draft form pending executive approval. This package includes measures previously proposed as well as two new measures,

115. **Finding no. 7: CSIS and the RCMP do not have a shared vision or joint long-term strategy for addressing the threat to national security posed by**

Recommendation no. 4: NSIRA recommends that CSIS and the RCMP develop a properly resourced joint strategy to address the threat posed by

In accordance with the vision set out in the Operational Improvement Review, the strategy should consider the full range of tools available to both agencies.

V CONCLUSION

116. In planning this review, it was decided to use the investigations of both CSIS and the RCMP as a lens through which to examine the general state of the CSIS-RCMP relationship, and in particular to see how the two organizations are managing the obstacles of the intelligence-to-evidence problem by means of the One Vision 2.0 framework.

117. As with the choice of any specific subset of activities, it is understood that the subset may not be perfectly representative of the broader whole. Nonetheless, this review encompassed a wide range of operational activities over several years, and included an examination of the headquarters dimension of the relationship. At no point was NSIRA informed that the CSIS-RCMP relationship was exceptional or unusual, for better or for worse, compared to the relationships that exist elsewhere in Canada.

118. No doubt each province and each investigation has its own particular dynamics and challenges, and the strength and effectiveness of the CSIS-RCMP relationship in different regions will fluctuate as key individuals change over time. But NSIRA was given no reason to believe that the high-level issues it observed were unique or to the investigation.

119.

Regardless, the situation raises the question of why A full answer to that question was beyond the scope of this review, but NSIRA did learn of several challenges facing the investigation that have likely contributed.

- **Resources:** NSIRA heard from that it must prioritize only the most urgent for its part, also noted that it lacked the resources to mount large-scale and sustained investigations of issues like that do not appear to pose an urgent threat to Canadian life.
- **Intelligence-to-evidence:** Despite the recent problems CSIS continues to gather intelligence on the threat activities of While CSIS has kept the RCMP generally informed of its investigation through One Vision 2.0 meetings, very little information has been formally disclosed to the RCMP, and front-line RCMP investigators derive little benefit from CSIS's work. As noted above, this is not the 'fault' of either CSIS or the RCMP, but reflects a shared understanding that CSIS information puts RCMP investigations at risk of failure during the trial phase given the need to protect CSIS sources and methods.

120. An ordinary Canadian could be forgiven for wondering at a system in which one government agency in Ottawa has amassed a large collection of intelligence on a threat, while across town another government agency – one tasked with investigating and arresting suspected criminals – by and large does not receive and/or believes it cannot use that intelligence. Surely this state of affairs could be improved.

121. The intelligence-to-evidence problems facing CSIS and the RCMP are longstanding, and improvements are overdue. The present Operational Improvement Review is an ambitious re-think of the assumptions that have long guided the CSIS-RCMP relationship. NSIRA remains seized of the intelligence-to-evidence issue and its impact. At the appropriate time in the coming years, NSIRA will launch a review of CSIS and the RCMP's implementation of the Operational Improvement Review in order to assess progress and take stock of the results.

The Federal Court and NSIRA

122. In May 2020, the Federal Court rendered a decision in which it concluded that CSIS had failed in its duty of candour to disclose

123. In its May 2020 decision, the Court recommended that a review body investigate the systemic, governance and cultural shortcomings and failures that resulted in CSIS having and the related breach of the duty of candour.[167] In response, the Minister of Public Safety and Emergency Preparedness and the Minister of Justice referred the issue to NSIRA under paragraph 8(1)(c) of the *NSIRA Act*.[168] NSIRA has since begun this review, both in response to this ministerial referral and under NSIRA's own independent review authority. The review is being led by NSIRA members the Honourable Marie Deschamps and Professor Craig Forcese.

124. NSIRA considers the situation with to be closely connected to the more general failures cited by the Federal Court in its recent decision. NSIRA's review will examine CSIS's culture and practices regarding candour as they relate to particular.

[167] 2020 FC 616, May 15, 2020.
[168] *Joint Statement by Minister of Public Safety and Minister of Justice and Attorney General of Canada on Federal Court en banc matter*, July 16, 2020.

ANNEX A: Scope and Methodology

1. NSIRA decided to anchor its review in the national security and intelligence activities of a specific CSIS region, namely After a series of preliminary briefings, NSIRA reviewers selected investigation into as a lens through which to examine CSIS's working relationship with its key domestic partners. This decision was made in part because the investigation of is one of investigations, and in part because CSIS collaborates extensively with other agencies on this investigation.

2. Ultimately, NSIRA chose to focus on the relationship between CSIS and the RCMP, not only because the RCMP is CSIS's key partner on the investigation, but also because their relationship is governed by a detailed framework, and because the relationship between CSIS and the RCMP is important, as noted It would therefore be in the public interest to undertake an in-depth case study to better understand how, today, the relationship functions.

3. NSIRA used several lines of evidence to ensure that the review's findings are supported by multiple sources wherever possible. Reviewers submitted requests for information and documentation to both CSIS and the RCMP and analyzed this documentation. At CSIS, reviewers sought, retrieved and reviewed documents independently within CSIS's databases, to ensure a complete and clear record of activity.

4. Briefings began in May 2019 and concluded in March 2020; they are listed in Annex B, below. In December 2019, NSIRA travelled to for several days of meetings with both

5. The core review period was from January 1, 2017, to October 31, 2020, although reviewers examined documentation that fell outside this period where it was deemed necessary to fully understand relevant issues.

6. Some avenues of review were curtailed by the COVID-19 pandemic, which limited the ability of reviewers to access classified documents starting in March 2020. NSIRA will pursue these lines of inquiry in future reviews.

7. NSIRA capitalized on its visit to interview CSIS operational employees directly regarding the impact of the on their day-to-day operations. As was not the main focus on this review, the discussion of is found at Annex C.

ANNEX B: Briefings

- 2018-11-01: Briefing from CSIS Deputy Director of Operations Secretariat
- 2019-05-16: Briefing from CSIS
- 2019-07-09: Briefing from CSIS Intelligence Assessments Branch
- 2019-07-12: Briefing from CSIS on CSIS's Relationship with RCMP
- 2019-09-16: Briefing from CSIS on reviewed investigation
- 2019-09-17: Briefing from the Canada Border Services Agency on its operational relationship with CSIS, particularly
- 2019-10-10: Joint briefing from the RCMP and CSIS on the Operational Improvement Review
- 2019-10-21: Briefing from the RCMP on related investigations and the RCMP-CSIS relationship
- 2019-11-28: Briefing from CSIS on warrants related to the investigation under review
- 2019-12-02: Briefing from CSIS on
- 2019-12-09, 2019-12-11, 2019-12-12: Briefings from
- 2019-12-10: Briefings from RCMP
- 2020-02-27: Briefing from CSIS
- 2020-03-11: Briefing from CSIS Intelligence Assessments Branch

ANNEX C:

1. *Observation* was implemented without adequate consideration of its effect on CSIS personnel and operations. The resulting internal disruption

Introduction

2. One of the topics NSIRA examined over the course of this review was the effect of on CSIS personnel and operations, particularly

3. NSIRA's predecessor organization, the Security Intelligence Review Committee (SIRC), reviewed in 2017, at which time the new model had been rolled out and was only in the process of being implemented, but before firm conclusions about its consequences could be drawn.[169] In April 2019, a CSIS internal evaluation examined and included extensive observations and its effects.[170] NSIRA has read this report, and has drawn on its insights as part of this review. A comprehensive examination of was beyond the scope of this review, however.

4. NSIRA received a briefing from headquarters on and also took advantage of its travel as part of this review, to conduct its own interviews with CSIS operational employees in order to frame its own understanding. Specifically, NSIRA interviewed different groups of CSIS operational employees and their managers specifically The results of these interviews were broadly congruent with the results of the CSIS internal evaluation.

Background

5. has its origins in CSIS's 2010 Business Modernization Project (BMP), which discussed possible changes to model common within CSIS at the time.

6. Internal deliberations following the BMP resulted in the proposal of a new model for CSIS operations

169
170
171
172

7. This new model was piloted for six months
An internal report on the results of the pilot was generally positive, but noted a number of areas where more work was needed. Internal feedback recommended a gradual roll-out and highlighted the need for broader changes in order to accommodate the new model. In the end, was quickly rolled out to all regions in late 2015 without addressing many of the issues raised.[174]

Impact

21. The dislocation that began with the sudden roll-out of has not entirely abated. The CSIS internal evaluation and NSIRA's own interviews confirm that has been the cause of anger and frustration for many IOs. Anecdotal reports again suggest that has significantly damaged the morale of many of those affected.

The CSIS Response

22. CSIS leadership is aware that has fallen short of its goals. A memorandum dated September 13, 2019, signed by the Directors General of each CSIS region (the Regional DGs or RDGs), conceded that 'has not delivered the expected level of benefit

23. In response, the RDGs recommended changes to address the more urgent problems while retaining the positive aspects. In particular, they proposed

NSIRA understands that some regions have since adopted these changes.

25.

The recent changes may have mitigated some of the more pressing concerns but important broader issues remain unresolved. It is unclear why needed to be implemented as quickly as it was,

With a more considered deployment, most of the initial issues caused by could presumably have been avoided or at least anticipated and proactively mitigated.

26

As such, the problems revealed by this review are concerning to NSIRA.

NSIRA may undertake a more comprehensive review of and associated issues in future to assess CSIS's progress in addressing these outstanding issues.

ANNEX D: Findings and Recommendations

Findings

1. Since 2019, there have been significant caps in CSIS's intelligence collection on the threat posed by

2. Reliance on makes CSIS's investigation into

3. A lack of usable and compatible secure communications tools is making CSIS-RCMP de-confliction excessively burdensome and time-consuming.

4. Despite persistent challenges related to information sharing and governance structures, have developed a strong relationship that has fostered effective tactical de-confliction .

5. One Vision 2.0 has left fundamental issues related to the intelligence-to-evidence problem unresolved. In the case of despite frequent verbal exchanges between CSIS and RCMP headquarters, CSIS's formal disclosures of information have been limited and not always useful. CSIS intelligence has not been shared or used in a way that has significantly advanced the RCMP's investigations.

6. The Operational Improvement Review has the support of senior management of both CSIS and the RCMP and work is underway to assess and implement its recommendations.

7. CSIS and the RCMP do not have a shared vision or joint long-term strategy for addressing the threat to national security posed by

Recommendations

1. NSIRA recommends that CSIS invest the resources needed to avoid having to

2. NSIRA recommends that CSIS and the RCMP prioritize the deployment of usable and compatible secure communications systems in order to make regional de-confliction more efficient.

3. NSIRA recommends that both CSIS and the RCMP continue to prioritize the timely implementation of recommendations from the Operational Improvement Review (OIR) in order to help address the operational shortcomings reported by the OIR and further illustrated in this review.

4. NSIRA recommends that CSIS and the RCMP develop a properly resourced joint strategy to address the threat posed by In accordance with the vision set out in the Operational Improvement Review, the strategy should consider the full range of tools available to both agencies.