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

Review of Public Safety Canada and the Canadian Security Intelligence Service's Accountability Mechanisms

NSIRA // Review 22-12 TOP SECRET//CEO

Table of Contents

List of Acronyms

CBSA Canada Border Services Agency

CAF Canadian Armed Forces

CSIS Canadian Security Intelligence Service (or Service)

DDO Deputy Director Operations

DM Deputy Minister

DOJ Department of Justice

GAC Global Affairs Canada

GC Government of Canada

IG Inspector General of CSIS

MD Ministerial Direction

[redacted]

NSIA National Security and Intelligence Advisor to the Prime Minister

NSIRA National Security and Intelligence Review Agency

ORA Operational Risk Assessment

PCO Privy Council Office

PS Public Safety Canada

RCMP Royal Canadian Mounted Police

SIRC Security Intelligence Review Committee

Executive Summary

This review stems from a September 2022 referral by the former Minister of Public Safety (PS). The Minister requested that NSIRA evaluate whether the Canadian Security Intelligence Service's (CSIS or the Service) risk assessment model, Ministerial Direction (MD) and other information sharing mechanisms enable the Minister to effectively discharge their responsibilities for CSIS. Ministerial concerns about the adequacy of such mechanisms arose from CSIS's [participation in...] an operation which prompted considerable deliberation within Canada's national security community and direct intervention by [*]

Of the four current MDs to CSIS, three are relevant to accountability for operations: Threats to the Security of Canada Directed at Parliament and Parliamentarians (2023); Operations (2023); and, Accountability (2019). Responding to the Minister's referral, NSIRA examined CSIS's implementation of these MDs, including its establishment of an interdepartmental consultative process to engage Public Safety Canada (PS), Global Affairs Canada (GAC) and the Department of Justice (DOJ) in assessing the reputational, foreign policy and legal risks of the Service's proposed operations. NSIRA also decided to review the aforementioned CSIS [redacted] operation.

NSIRA found that the decision to halt this active CSIS operation [redacted] was not made by the CSIS Director under section 6(1) of the CSIS Act, and for which there is no written record of a direction coming from the Minister of Public Safety under sections 6(1) or 6(2) of the CSIS Act. Moreover, [**] to halt this active operation created unnecessary danger for the CSIS team [redacted] and caused harm to Canada's international reputation.

While the Minister is accountable for CSIS activities, both PS and the Service must ensure their briefings to the Minister support this accountability. And on this point, the review found that PS and CSIS failed in their responsibility to provide timely and accurate information to the Minister about [redacted] human source [redacted] operation. NSIRA attributes these shortcomings to PS willingly remaining dependent on CSIS to identify and receive relevant information, which inhibits PS's ability to prepare independent advice to the Minister about the activities and operations of CSIS.

NSIRA found that multiple MDs to CSIS are subject to inconsistent and contradictory interpretation by those responsible for their implementation. Moreover, NSIRA found that when preparing MDs to CSIS, PS insufficiently consulted with GAC and CSIS.

CSIS's risk assessment process has evolved to become the central mechanism for planning operations and managing associated risks, and, while it is generally effective, it lacks clear guidance to employees on when risk should be reassessed as operations

evolve. For foreign policy risk assessments, GAC and CSIS do not have a shared vision with respect to the role of GAC in this process.

NSIRA also found that legal advice is often absent from the final risk assessment record for CSIS operations. Moreover, the scope of legal considerations within these legal risk assessments is under-inclusive.

PS's reliance on CSIS to identify relevant information is most plainly seen in the inadequacy of PS's contribution on the preparation of reputational risk assessments. Although CSIS must retain management and control of its operational activities, this does not displace PS's responsibility to ensure the Minister has all the information needed to make informed decisions and fulfill their accountability requirements. The [redacted] operation – which was exceptional but not novel – demonstrates the negative consequences of PS's current approach.

In total, the review makes eleven findings which are addressed through six recommendations, which include that:

1. Whenever there is a decision affecting an active CSIS operation, which is not made by the Director of CSIS or their delegates, it must come as a direction from the Minister of Public Safety under section 6(1) of the CSIS Act and should be accompanied by a written record in keeping with section 6(2);
2. The Minister of Public Safety take action to ensure that the Deputy Minister obtains any information required to fulfill their responsibility to provide independent advice to the Minister about the activities and operations of CSIS;
3. The Minister of Public Safety consolidate ministerial directions into clear, concise and harmonized instruments that are derived from meaningful consultation among those responsible for their implementation;
4. CSIS, in consultation with DOJ and GAC, ensure that legal risk assessments are comprehensive and memorialized in writing;
5. Any pending changes to CSIS's risk assessment process maintain a robust consultation and information sharing mechanism between GAC and CSIS; and,
6. PS and CSIS develop a more robust consultation mechanism for reputational risk assessment for CSIS operational activities, and that these assessments account for the risk of discrediting the Government of Canada.

1. Introduction

Authority

1. This review was conducted under the authority of paragraphs 8(1) (a), (b) and (c), and 8(2.1) (a) of the *National Security and Intelligence Review Agency Act* (NSIRA Act).

Scope of the Review

2. This review examined the Canadian Security Intelligence Service's (CSIS or the Service) risk assessment model, Ministerial Direction (MD) and other information sharing mechanisms to determine if decision makers, including the Minister of Public Safety (PS), are provided with accurate and timely information. As part of this assessment, NSIRA examined the Service's risk assessment consultations with Public Safety Canada (PS), Global Affairs Canada (GAC), and Department of Justice (DOJ). The Service's [redacted] program was narrowly reviewed with respect to MD and risk, and limited to the context of a specific CSIS [redacted] operation [redacted] The time period for review spanned January 1, 2015 to July 31, 2023.

Methodology

3. NSIRA had direct access to CSIS information holdings, remote portal access to GAC information, submitted 27 requests for information, attended 13 briefings and conducted 17 interviews. The information reviewed from the four departments included: relevant legislation, MDs, policies, procedures, [redacted] files, presentations, briefing notes, meeting summaries, legal advice and opinions, cooperation frameworks/mechanisms, and administrative and operational correspondence (e.g. memos, emails, and text messages).

4. For calendar year [redacted], NSIRA assessed over 50 ministerial memos and supporting documentation; [redacted] of these memos involved 'high-risk' notifications to the Minister of PS. NSIRA additionally examined approximately 100 risk assessments from a variety of operational environments, including [redacted] [operational details...] risk assessments,

as well as a number of operations within Canadian fundamental institutions (i.e. academia, trade unions, government and political institutions, and the media). Finally, NSIRA reviewed all of GAC's [redacted] foreign policy risk assessments (i.e. [redacted] total, [redacted] assessed as high risk).

Review Statements

5. NSIRA found that its expectations for responsiveness by all reviewees during this review were met. NSIRA was satisfied by the proactive disclosure of relevant information by CSIS and GAC, and thanks employees from DOJ, PS and CSIS who volunteered to participate in NSIRA interviews.

6. NSIRA was able to verify information for this review in a manner that met expectations.

2. Background

The Referral – Did the Minister have the necessary Information?

7. This review stems from a referral to NSIRA by the former Minister of PS on September 15, 2022. The Minister asked NSIRA to evaluate whether the Service's accountability mechanisms provide sufficient information to allow the Minister to effectively discharge their role as Minister responsible for CSIS. Concern on the adequacy of such mechanisms arose from [redacted] operation conducted by CSIS in [redacted] the circumstances surrounding this operation [redacted] led to extensive debate within Canada's national security community and direct intervention by [political] and ultimately, was the catalyst for the referral to NSIRA.

8. In his letter, the Minister requested that NSIRA examine MD to CSIS, the Service's risk assessment processes [redacted] program, as well as implementation of previous Security Intelligence Review Committee (SIRC) recommendations to CSIS, and whether any further changes were required. These questions informed NSIRA's scoping of the review.

9. To appreciate the reasoning behind the Minister's referral to NSIRA, it is first necessary to know the contextual underpinnings which led CSIS [to [redacted]

carry out this activity...] as well as understand specific details about the operation.

The Source, the Operation, and the Halt

10. [background on operation...]

11. SIRC examined this case in detail provided findings and recommendations aimed at addressing a number of interrelated issues, including: legality of operations MD, risk management, internal oversight, identity management, domestic and foreign partnerships, loss of operational environments and foreign strategic orientation. CSIS accepted all of SIRC's recommendations, and these improvements were subject to additional review in subsequent years.

12. The story commences in when CSIS first learned of [information that required the planning of a specific category of operation...] CSIS started working with domestic and foreign partners operation involving CSIS

13. the Service informed both the Minister and PS just over two weeks prior to the scheduled operation, [and on other pertinent details related to the activities...] The Minister and PS raised no objections to proceed with the operation. Everything proceeded as planned, including CSIS team

[redacted]

14. [Government and political-level stakeholders met to talk about the operation...] [redacted] The ensuing debate resulted [**] [redacted] to CSIS to halt – mid-operation [redacted] activities in [redacted] This decision needlessly placed [redacted] officers in danger, and raises serious concerns regarding CSIS's accountability mechanisms. Ultimately, the operation was allowed to proceed by [redacted] after a delay [redacted] The governance of this case will be examined throughout the analysis in this report.

3. Findings, Analysis, and Recommendations

Accountability and Consequences for Halting the [codename] Operation

Finding 1. NSIRA found that a decision was made to halt an active CSIS operation overseas that was not made by the CSIS Director under section 6(1) of the CSIS Act, and for which there is no written record of a direction coming from the Minister of Public Safety under sections 6(1) or 6(2) of the CSIS Act.

15. Critical to the principle of responsible government is that ministers are accountable to Parliament for the actions of departments and agencies under their care. For the Minister of PS, this responsibility extends to exercising leadership at the national level relating to public safety and for coordinating the activities of a portfolio which includes 66,000 employees and a $9 billion total annual budget for the Royal Canadian Mounted Police (RCMP); CSIS; the Canada Border Services Agency (CBSA); the Canadian Firearms Centre; the Correctional Service of Canada; and the Parole Board of Canada.

16. Given the size and scope of responsibilities for this portfolio, it would be impractical to presume that the Minister has knowledge of every issue. However, given that claims of ignorance are antithetical to the principle of responsible government, the Minister is accountable for every matter within the scope of their portfolio, whether or not they have knowledge of it. Most importantly, the Minister must take appropriate corrective action to address problems once informed of them by the public service, principally through the appropriate Deputy Minister (DM).

17. The *Public Safety Act* imposes broad national security responsibility on the Minister of PS. For example, section 4(2) provides that "the Minister is responsible for exercising leadership at the national level relating to public safety and emergency preparedness" and therefore, when considering the activities of CSIS, it is expected that the Minister will need to balance a wider set of interests in certain circumstances. This could include, for instance, whether the activity in question occurs in whole or in part outside of Canada, or if it engages the mandate of another Minister. This in turn requires that the DM of PS be sufficiently informed of all relevant information to advise and support the Minister.

18. Section 6(1) of the CSIS Act states that the Director, under the direction of the Minister, has the control and management of the Service. Approval [redacted] CSIS human source is made by the CSIS Deputy Director Operations, as per policy. In practice, the Minister has a more limited role with respect to these operations. For example, in addition to being notified of high-risk activities pursuant to MD, the Director's classified annual report is also to inform the Minister of [redacted] human source [redacted]

19. The [redacted] to halt [redacted] raises questions about the web of accountability mechanisms that connect the Minister to CSIS. According to document review and NSIRA interviews, the direction to halt [redacted] operation occurring [redacted] was the result of [political-level discussions...] [redacted] and first came from the National Security and Intelligence Advisor to the Prime Minister (NSIA) to the Director of CSIS. [redacted] team [redacted] meanwhile, was advised that "further to political-level direction," the operation was "delayed". Crucially, the CSIS team was not aware of when [redacted] activity would be permitted to resume, if at all.

20. The review revealed that CSIS senior officials had difficulty in grappling with [redacted] to halt the operation; so much so, in fact, that management and control of the operation appeared to cease functioning properly. The Director of CSIS, for instance, evidently no longer had decision making control over the active operation, when on [redacted] he sent an email to senior officials within key security and intelligence portfolios stating: "time is quickly running out and the situation is getting much more tense on the ground. We need a decision tomorrow."

21. Compounding the confusion was uncertainty as to who had authority to resume an active operation once [redacted] was involved. [redacted]

[internal discussions at CSIS about operation...]

22. The CSIS Deputy Director approved the operation in writing However, there is no written record that captures the decision to halt the operation The same is the case for the decision to proceed with the operation If the decision is not made by the CSIS Director or delegates, it must be the Minister who provides the appropriate direction. In law and by convention, the Minister will always be held accountable for the activities of CSIS, regardless of whether [*] has made the actual decisions directing these activities. While such memorialization is undertaken for routine Ministerial decision making, such as approving the submission of warrants, no system exists for exceptional circumstance

Recommendation 1. NSIRA recommends that whenever there is a decision affecting an active CSIS operation, which is not made by the Director of CSIS or their delegates, it must come as a direction from the Minister of Public Safety under section 6(1) of the CSIS Act and should be accompanied by a written record in keeping with section 6(2).

Finding 2. NSIRA found that [*] halted an active operation, creating unnecessary danger for the CSIS team and caused harm to Canada's international reputation.

23. Regularized processes assist in reducing operational risks. When predictable decision-making practices become strained or are absent, individuals become increasingly prone to precipitous decisions, which can result in serious detrimental consequences. operation drives home the necessity of thorough operational planning and comprehensive consultation to obtain required approvals and necessary support prior to operational execution.

24. [**] to halt an active and sensitive CSIS operation produced damaging consequences. CSIS, had accepted [certain preconditions...] in advance of the

operation. made clear that a failure to would result in

25. The CSIS team also believed – reasonably in NSIRA's view – that safety was in jeopardy. perspective, the operational delay undermined confidence in the Service's adherence [to the operational conditions] The CSIS team told NSIRA that they felt abandoned and, they believed that the absence of a Government decision "was a decision" (i.e. the Government would allow leaving no choice but Facing this untenable situation, the CSIS team felt forced to plan alternative actions to help ensure their own, safety.

26. As serious as the situation appeared to be when the operation was halted, the stakes were raised further after the team of CSIS officers conducting the operation agreed that Not only would this have caused grave diplomatic harm to Canada's relationship but it is likely that the resulting would have also signalled that CSIS could not to be trusted Such an outcome would have also potentially created legal and other accountability issues for CSIS, its officers, and the GC.

27. CSIS operational employees informed NSIRA that this operation's legacy has had a chilling effect on CSIS-PS relations. CSIS-HQ rejects this perspective, claiming instead that there continues to be close collaboration and frequent information sharing with counterparts at PS. Irrespective of which perspective is accurate – CSIS employees or management – this review makes the case for PS to take on a much more robust role in upholding its responsibilities in relation to CSIS. If PS is prepared to adopt this stance, there will be opportunity for more timely and thorough discussions with CSIS on complex operations, with direct benefit to ministerial accountability.

Responsibility for Briefing the Minister [about codename]

Finding 3. NSIRA found that Public Safety and CSIS failed in their responsibility to provide timely and accurate information to the Minister of Public Safety about [redacted] human source [redacted] operation.

28. The Minister is accountable, yet PS and CSIS are responsible for sufficiently briefing the Minister. In addition to certain provisions within the CSIS Act that require engagement of the Minister, the 2015 MD on Operations and Accountability, [redacted]

> [quote from MD...] [redacted]

29. PS and CSIS use a variety of communication methods to keep the Minister of PS apprised of CSIS's activities. The Director's annual report to the Minister provides the most comprehensive *ex post facto* coverage of CSIS activities. Other communication tools are used to help ensure compliance with MD's stipulation to notify the Minister of source operations that *may engage* in activities that could discredit the Service or the Government. This includes regular classified briefings by CSIS, attended by PS and other portfolio representatives, as required. These engagements may include updates on the minutia of sensitive source operations, to information of a more strategic nature. There are also briefing packages, information notes, presentations by subject matter experts, as well as private discussions, either in person or by secure phone, between the Minister and the DM and/or CSIS Director. Given the operational tempo of some national security matters, some exchanges involving the Minister are not formally scheduled (e.g. they may occur adjacent to other briefings, during foreign and domestic travel, and on an urgent basis).

30. Throughout this review NSIRA listened to the perspectives of those most involved in ensuring that the right information is provided to the Minister at the appropriate time, and with proper context. NSIRA interviews revealed that day to day working realities are not conducive to reflective thought, with one individual describing their role as "air traffic controller," which requires prioritizing a large volume of information destined for the Minister. Interviewees also described dealing with the

realities of limited ministerial availability; having to place trust in a complex bureaucracy; comprehending incomplete and/or inaccurate information as part of the realities of national security; and limited technological options for sensitive transactions when the Minister is not in Ottawa.

31. Despite the challenges, PS and CSIS are rarely unaware of potentially relevant issues that should be briefed to the Minister. CSIS is aware that certain MDs impose a notification requirement on the CSIS Director to proactively identify known issues; this extends to when a new Minister is transitioning into the role. The MD on Accountability requires the Director to advise the Minister of issues on a case-by-case basis when necessary. A case of necessity could include providing a Minister with context on past operations that may become matters of litigation and/or sources that might be in peril. For example, CSIS has acknowledged to NSIRA that the Minister of PS could have been briefed at an earlier point in his tenure [about relevant details...]

32. It is also the case that PS was aware of the historical, legal, reputational and foreign policy issues and possessed sufficient information to expect challenges As such, the DM of PS had an equally compelling positive obligation to independently brief the Minister about these legacy implications when the Minister assumed their portfolio responsibilities. This is irrespective of whether or not CSIS, at the time, felt that this information was relevant to raise to the Minister.

33. While it is important to provide information to the Minister on the ongoing risks associated with legacy operations, even more critical is ensuring timely and accurate reporting on contemporary matters. This was particularly evident during the operation, where the Minister was initially informed in a classified briefing by CSIS on – the same day that PS was first made aware. There is no official record for the Ministerial briefing on Based on interviews with those who interacted with the Minister, CSIS provided reassurance that the operation was not unusual, and pointed out that the operation was not assessed as 'high risk' (which meant there was no obligation within MD to notify the Minister). However, in the opinion of one senior PS official, the limited time between being made aware of the planned operational execution did not provide PS with sufficient 'lead time' to prepare and independently provide advice, and ultimately, led the Minister to feel like "his hands were tied".

34. Contrary to the view of PS, CSIS maintains that "extensive efforts were made to ensure that the Minister and key partners were aware [redacted] during a compressed period of time" when the operation itself was being planned and executed. CSIS also defends the delay in informing PS and the Minister until it had [redacted] which the Service did not receive until [redacted] Finally, CSIS points to [redacted] the absence of adequate briefing-up by the Privy Council Office (PCO) to the Prime Minister (in advance [redacted] as factors that contributed to halting the operation.

35. The account by CSIS is not supported by the documentary record. CSIS knew well in advance [redacted] [of the execution of this category of operation and of pertinent information that was relevant for ministerial consideration...] [redacted]

36. [redacted] CSIS spent [redacted] advancing work on [redacted] with many other Canadian departments/agencies – including agencies within the public safety portfolio – as well as with international partners. Therefore, excluding PS was a choice. For instance, when NSIRA asked why PS was not involved in these discussions, CSIS stated that it was due to PS being policy focussed, not operationally engaged.

37. PS does not dispute CSIS's interpretation of its role. For example, in answer to NSIRA's questions, PS noted a preference to refrain from speaking about CSIS operational matters unilaterally to the Minister. In general, PS aims to have the DM and Director collaborate, as "would be expected by the Minister". However, the roles of PS and CSIS are not synonymous; PS has a wider mandate, and this may, on occasion, necessitate unilateral PS-Ministerial discussions touching on CSIS activities. The desirable collaborative approach must not come at the expense of independent advice from PS. The alternative risks perfunctory interactions between CSIS, PS and the Minister which are a *fait accompli*.

38. CSIS's claim that the Prime Minister was inadequately briefed understates the matter; there is no indication that the Prime Minister had any awareness of this operation. With sufficient forewarning and preparation, [the political-level may have decided...] not to halt this operation. For instance, the Information Note CSIS provided to the Prime Minister on presented a more robust argument on the merits of [of a particular approach to the operation] than that provided to the Minister of PS on

39. It was not the timing of this operation that led to the issues NSIRA observed with this case, but rather, the poor quality of operational preparation and consultation. PS and CSIS had an advance window to prepare it is reasonable to expect that broad consultation would have taken place among Government stakeholders.

40. Even once the Minister was aware of the operation, PS and CSIS did not provide the Minister with sufficient information. When CSIS briefed the Minister it neglected to inform the Minister [on all details] At the time, CSIS believed that this information was not relevant, and PS was in no position to provide an independent appraisal. [after other circumstances transpired...] the Minister raised additional concerns about reputational harm to the Government, and the thoroughness of these initial briefings.

41. Finally, CSIS's memo addressing which included a covering PS note as well as additional background materials, still provided the Minister with incomplete information.

42. The memo's description [redacted] failed to convey [redacted] had identified a number of CSIS activities as problematic, and potentially unlawful. Of note, [redacted] was that the CSIS Director had not complied with the then-2008 MD for Operations because he had failed to notify the Minister [redacted] The [redacted] memo should have accurately reflected previous deficiencies in accountability to guide the Minister's scrutiny of CSIS's proposed operation.

Public Safety's Role in Relation to CSIS

Finding 4. NSIRA found that Public Safety willingly remains dependent on CSIS to identify and receive relevant information, which inhibits Public Safety's ability to prepare independent advice to the Minister about the activities and operations of CSIS.

43. PS's role in providing independent advice to the Minister on the activities and operations of CSIS is neither clearly articulated in legislation, nor plainly captured within relevant policy instruments. Rather, such expectations are to be found in parliamentary discussions leading to creation of the CSIS Act, as well as associated commissions of inquiry. As reflected in its statutory framework, PS has an important complementary role to CSIS in providing the Minister with information needed to discharge ministerial leadership responsibilities in national security matters. For a brief synopsis of some of the more salient points in this respect, please refer to Annex B.

44. A recognition for the need for departmental scrutiny of the Service initially led to the creation of the Office of the Inspector General of CSIS (IG). Described as the "minister's eyes and ears," the IG was expected to monitor CSIS compliance with the law, ministerial direction, and operational policies, as well as comment on the Service's overall performance. The IG reported directly to the DM of PS, and was entitled to have access to any information under the control of the Service, similar in all respects to the powers granted to SIRC, and now NSIRA. In 2012, the IG was eliminated, which created a gap in PS's information on and awareness of CSIS activities.

45. In September 2019, the Minister of PS issued a standalone MD to CSIS for Accountability. The intent of the new MD was to reinforce the Minister's expectations of CSIS with respect to compliance with the law, duty of candour to the Federal Court, and particularly the duty to inform the Minister "of any such

matter as is relevant to enable" the fulfillment of the Minister's accountabilities. To compensate for the information deficit created by the loss of the IG, the MD also instituted a 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* (Cooperation Framework) between PS and CSIS aimed at formalizing information transfer for accountability purposes.

46. From PS's perspective, the 2020 Cooperation Framework has satisfactorily addressed the information deficit. NSIRA observed extensive information sharing through this process, facilitated through quarterly meetings between PS and CSIS. This is in addition to the frequent exchange of classified memos, emails and phone calls that occurs between PS and CSIS on all matter of issues.

47. Determining whether the CSIS Act, MD on Accountability, and the Cooperation Framework have created an information sharing regime that satisfies the needs of PS and the Minister is a central preoccupation of this review. Although each instrument provides gateways for information exchange from CSIS to PS, the overall regime has not compensated for the loss of the most important statutory authority possessed by the former IG: principally, unrestricted access to CSIS's information holdings. Instead, CSIS controls information provision to PS. There is no indication that CSIS is deliberately constraining the ability of PS to prepare independent advice to the Minister. However, PS deference to CSIS viewpoints and overreliance on CSIS selected information and final products, cumulatively diminishes the DM of PS's ability to provide robust independent advice to the Minister.

48. For example, PS does not have direct access to human source files, despite CSIS being first and foremost a HUMINT agency. PS also does not have routine access to CSIS operational risk assessments, nor has it taken measures to demand such access or availed itself when access has been granted. To illustrate, PS made three requests to CSIS for a copy of [redacted] risk assessment, the first [redacted] and a second and third time [redacted] The Service told NSIRA it granted PS an opportunity to see this document, with the proviso that, due to its sensitivity, the document could only be examined at CSIS HQ. At time of writing, PS had yet to examine this assessment.

49. Except for what is explicitly required by law or under the authority of MD, PS is reliant on CSIS to proactively provide information that the Service determines may require PS and/or Ministerial attention. As acknowledged by PS:

> (The department) must have enough information to inform the Minister; we cannot report what we do not have, or what we have only heard informally or through quick verbal exchanges.

50. When asked why it does not have proactive access to information, PS highlighted three considerations: first, the importance of maintaining CSIS information security; second, the Service's operational tempo and limited PS resources would make timely assessment of additional information difficult; and finally, CSIS provides higher level information through the Cooperation Framework in accordance with PS's policy and guidance role.

51. From CSIS's perspective, unrestricted access to all of its holdings would be required for PS to be more active in the Service's operations. CSIS believes that such unrestricted access would be inefficient, unnecessary, constitute a security risk, and would duplicate CSIS advice already provided to the Minister and copied to the DM of PS.

52. Having considered both CSIS and PS's responses, these security and resource concerns are unpersuasive. First, the onus is on both PS and CSIS to establish a security infrastructure that facilitates access, even for the most sensitive of information. PS does not require unrestricted access to all CSIS holdings. Rather, it only needs access to those holdings which are necessary in the given circumstance to provide independent advice on the proposed activity beyond what was initially furnished by CSIS. Security controls already exist at CSIS, as do mechanisms that audit for security policy non-compliance. Second, if ensuring adequate accountability requires additional resource investment, then this is something which can be addressed through budgetary requests.

53. Finally, the distinction between policy and operations, as conveyed by both PS and CSIS, is not a useful paradigm. This bifurcation of responsibility was rejected after careful consideration by the commission of inquiry that led to the creation of CSIS, the McDonald Commission, and is also not consistent with Parliamentary deliberations on the relationship expected of CSIS and PS (or the Solicitor-General's department, as it was originally known). See Annex B.

54. PS must be in position to brief the Minister of PS on the broader equities and interests that will inform their decision. To provide this advice to the Minister, PS must have access to the specifics of CSIS operations. Although CSIS must retain management and control of its operational activities, this does not displace PS's responsibility to ensure the Minister has all the information needed to make informed decisions and fulfill their accountability requirements. [redacted]

operation – which was exceptional but not novel – demonstrates the negative consequences of PS's current approach.

55. Ultimately, to ensure the provision of rigorous and genuinely independent advice to the Minister, the DM of PS must rely upon the assistance of well-informed departmental officials. It is therefore incumbent upon the DM to ensure these officials have access to CSIS operational information required to fulfill their duties. PCO provides some useful guidance on the role of the Minister vis-à-vis their Deputy Minister. For example:

> Depending on the portfolio, the Deputy Minister may also be assigned certain specific responsibilities by the Minister. In those cases, it is important that the Minister provide clear guidance to all agency heads on his or her expectations with respect to the role of the Deputy Minister. This role must not infringe upon the accountability of the agency head.[1]

56. To this end, the DM of PS already has tools available to further empower their employees in supporting ministerial accountability. The CSIS Act provides in subsection 7(3) that:

> The [DM PS] shall advise the Minister with respect to directions issued under subsection 6(2) or that should, in the opinion of the [DM PS], be issued under that subsection.

Recommendation 2. NSIRA recommends that the Minister of Public Safety take action to ensure that the Deputy Minister obtains any information required to fulfill their responsibility to provide independent advice to the Minister about the activities and operations of CSIS.

Ministerial Direction to CSIS

57. For the Minister of PS to be accountable to Parliament for the activities of CSIS, the Minister must be informed in advance of Service decisions and activities, and must not be left to simply react to them. Under section 6(2) of the CSIS Act, the Minister may take the initiative in developing and conveying expectations to CSIS by issuing written direction to the Director.

---

[1] "Guidance for Deputy Minister," Privy Council Office, found at: https///www.canada.ca/en/privy-council/services/publications/guidance-deputy-ministers.html#TOC1_4

Purpose and History

58. In the early years of the Service's history, MD played a crucial role in shaping CSIS's policy landscape, reflecting the Government's evolving position on what constitutes necessary reporting on, and controls for, the Service's operations and activities. Parliament encouraged the issuance of ministerial direction to CSIS, underscoring a key rationale for severing security intelligence from the RCMP: providing for detailed direction of intrusive intelligence activities without compromising police independence.

59. Throughout the 1990s, changes to ministerial direction were incremental. SIRC provided the catalyst for many of these modifications, for example highlighting in 1995 the Service's "seriously deficient" policy development for human sources. This deficiency was addressed, in part, by new MDs. Subsequent SIRC reviews focused on such matters as MDs for investigations on university campuses and investigations conducted under the CSIS Act's provisions on "subversion." Elsewhere, SIRC observed "policy lacunae" affecting CSIS's ability to translate MD into operational policy, such as "definitions of scope which are ambiguous as to when the Minister must be consulted or advised." By the end of the decade, there were twenty-eight MDs guiding CSIS.

60. In February 2001, the Minister issued an omnibus MD, which was modeled on the premise that most of the core elements of previous directions had been subsumed within applicable CSIS operational policies. Therefore, the Government determined that it was time to reduce and elevate MD to a more strategic level. Today, there are three MDs for CSIS that relate to accountability for operations: Threats to the Security of Canada Directed at Parliament and Parliamentarians (2023); Operations (2023); and, Accountability (2019).

Finding 5. NSIRA found that multiple Ministerial Directions to CSIS are subject to inconsistent and contradictory interpretation by those responsible for their implementation.

61. NSIRA observed that there are serious shortcomings in the current suite of MDs for CSIS. Crucially, there is no shared interdepartmental legal, policy or other documents that define the words and/or phrases used in MD. NSIRA was advised by PS to interpret these words according to their conventional meanings, and pointed to the fact that these are not drafted with legal precision. However, this review revealed that many of the words and/or phrases within MDs are prone to inconsistent interpretation by those responsible for implementation.

62. For example, within the 2019 MD the word 'consulted' is interpreted by PS as meaning *after-the-fact* for reputational risk assessment, while the exact word within the same MD is interpreted by GAC and CSIS as meaning *contemporaneously* for foreign policy risk assessment. Words like consulted, notification and advised are used across MDs in an interchangeable way. In the 2019 MD, for instance, it states that the Minister expects to be "consulted or informed" regarding any action on which a Deputy Head would normally involve his or her Minister; this, despite obvious differences in the conventional meanings for consult and inform.

63. In another example from the 2019 MD, the Service is to notify the Minister, "in advance," of operational activities where a novel authority, technique, or technology is used, or "prior to" activities where there is high risk. These sections of MD resulted in a number of informative interactions between NSIRA and interviewees responsible for providing information to, and interacting with the Minister. For instance, some interviewees struggled to articulate the expected role of the Minister when informed or notified of a CSIS activity before operational execution. Interviewees were inclined to point to sections of MD that clearly stipulated where the Minister was expected to 'approve' something (like in the case of a warrant). However, these same interviewees had difficulty in explaining why it was necessary to inform or notify the Minister before other operational activities transpired. The interviews revealed that, with exception where it is clearly stated otherwise, the role expected of the Minister is to be a passive recipient of information.

64. This was exemplified during the [redacted] operation. While being briefed by CSIS and PS, the Minister enquired what was expected of him, to which the Service explained that the briefing was for information only, although there may be a need [redacted] This answer to the Minister was consistent with a number of comments made by interviewees to NSIRA, where there appeared to be either hesitation, or an outright failure to understand the Minister's authority to direct the operation. The confusion which ensued once the [redacted] operation was halted is also reflective of this observation.

65. A similar issue exists within the phrase "in a timely manner" used in both 2023 MDs, in which there is no temporal deadline for when a Minister should expect to

[redacted]

receive information on ongoing high risk operational activities, or of "all instances of threats to the security of Canada directed at Parliament or parliamentarians". Certain CSIS employees interviewed by NSIRA believe that the Service's risk system is not dynamic – meaning that it cannot systematically provide ongoing operational risk assessments, regardless of this expectation. Moreover, 'all instances of threats' has no qualification, and is likewise prone to inconsistent interpretation, which means the Minister may not be fully informed.

66. Some interviewees had difficulty in explaining the key objectives of MD. The review identified that challenges in explaining aspects of direction may be the result of similar themes existing concurrently within multiple MDs. For instance, direction on risk is spread across the 2019 MD on Accountability and 2023 MD on Operations, and the preoccupations of the era in which each of these documents were written do not seamlessly weave together to create clear and succinct guidance.

Finding 6. NSIRA found that when preparing Ministerial Directions to CSIS, Public Safety insufficiently consulted with Global Affairs Canada and CSIS.

67. GAC was not sufficiently consulted on changes made to the 2023 MD on Operations affecting risk assessments for threat reduction measures, as well as approvals from the Minister of Foreign Affairs. GAC officials expressed the importance of maintaining visibility on and approvals for CSIS activities that engage their Minister's accountabilities. Likewise, while CSIS was consulted on the 2023 MD on threats directed at Parliament and Parliamentarians, CSIS reports that its input "was not necessarily provided to the Minister's Office" nor was it incorporated into the MD that was issued, despite the new guidance being very specific regarding operational expectations.

68. Finally, although PS and CSIS were involved in consultations involving changes to risk expectations within the 2023 MD on Operations, it is clear that these engagements were insufficient. Key stakeholders from both PS and CSIS could not explain to NSIRA the rationale for inclusion of entire sections of this MD, and how some of these expectations could be operationalized. [redacted]

Recommendation 3. NSIRA recommends that the Minister of Public Safety consolidate ministerial directions into clear, concise and harmonized instruments that are derived from meaningful consultation among those responsible for their implementation.

CSIS's Risk Assessment Process

69. Over the past thirty-five years, CSIS human sources have occasionally been involved in unlawful activities, [summary of other issues related to human sources...] In the past year alone, memos to the Minister of PS touched on high risk to either a legacy or active CSIS human source. [examples provided related to human sources...] it is appropriate that the identification, assessment and mitigation of risk has been a longstanding preoccupation for CSIS.

Purpose and History

70. The first significant step towards a modern risk system at CSIS was the result of a serious operational failure. [details on this operational failure...] SIRC would later assess that could not be attributed to any one action. Rather, a litany of factors were involved, including: CSIS's limited foreign operational capabilities, the lack of rigorous policies and procedures to manage foreign operations, insufficient risk management and training for and CSIS employees, and only a developing awareness of the challenges of conducting foreign operational activities with allies.

71. The operation resulted in the issuance of new MD in 2008 that emphasized the increased risk of CSIS's operations, and stipulated that the greater the risk associated with a particular activity, the higher the authority required for approval. This MD was silent on the process used to determine risk, reporting requirements to the Minister were vague, and participation from external stakeholders remained nascent.

72. The expectation for a "four pillar" risk analysis – i.e. legal, political/reputational, foreign policy, and operational – was first outlined within MD issued in 2015.

Following [redacted] SIRC recommended the development of an appropriate framework to capture risk considerations. This recommendation was addressed within the MD on Accountability in 2019, and in particular, provided further clarity on the external roles expected by DOJ for legal risk, GAC for foreign policy risk, and PS for reputational risk. [additional details on, and observations about MD...] [redacted]

Operational Pillar

Finding 7. NSIRA found that CSIS's risk assessment process has evolved to become the central mechanism for planning operations and managing associated risks, and, while it is generally effective, it lacks clear guidance to employees on when risk should be reassessed as operations evolve.

73. NSIRA examined a sample of over 100 risk assessments and supporting documentation and did not observe any non-compliance with law, MD or operational policies. Nonetheless, there remain some issues related to CSIS's operational risk pillar. For instance, stakeholder interviews with NSIRA pointed to an absence of formal processes to capture 'lessons learned' among regional counterparts and acknowledged the lack of standardized language in risk assessments. Moreover, the HQ center of excellence for risk does not have visibility on all risk assessments and lacks the technological ability for systematic trend analysis of the hundreds of risk assessments produced each year.

74. According to CSIS, outside of the [redacted] approval cycles for operations, operational risk assessments may be reassessed and adjusted for cause on an *ad hoc* basis. In the event of a change to the operating environment or operational activity, which may have an impact on risk, the employee responsible for the operation should inform the relevant risk expert in a timely manner, including providing an updated risk statement. Stakeholders, including GAC, are consulted as needed and if the resulting risk reassessment increases the overall risk, new approvals are required. However, CSIS currently lacks clear guidance to employees on when exactly risk should be reassessed outside of the standard [redacted] interval. A CSIS assessment on the state of the risk process raised similar concerns, and also pointed to an inconsistent understanding by management of the risk appetite for each of the four pillars of risk.

75. Recognizing the need for improvements, the Service launched project [redacted] which aims to create a new operational governance system, augmented by a modernized risk assessment system. Although in the early stages of development, NSIRA meetings and interviews with CSIS risk stakeholders suggest that the future system will reduce emphasis on narrative-type assessments and promote use of risk criteria, which are established reference points against which the significance of a risk is evaluated and measured. [redacted] [additional observations about risk system...] [redacted] The findings and recommendations contained within this report should inform project [redacted]

Legal Pillar

Finding 8. NSIRA found that legal advice is often absent from the final risk assessment record for CSIS operations.

76. The majority of risk assessments reviewed by NSIRA did not include written notation of DOJ consultation, and therefore, gave the impression that legal risk was under-assessed. DOJ as well as risk stakeholders across the Service, provided three key reasons for why written notation was absent from final risk assessments. First, the Service's justification framework under the CSIS Act for acts or omissions that would otherwise constitute offences under Canadian law has in some circumstances mitigated the identified legal risks. Second, DOJ is more frequently being consulted at an earlier stage of operational planning. This provides an opportunity to address legal concerns at earlier stages in the operational planning. Third, [redacted]

77. While earlier legal engagement is a positive development and may certainly assist in mitigating legal risk, the need for a documented legal risk assessment should always be required, even if this merely notes the reliance upon a foundational legal opinion. The risk assessment process provides managerial awareness of and approval for specific operations, and is a mechanism to capture the rationale for these decisions. Also, while the justification framework may address certain elements of legal risk, there are a number of other sources of legal risk. It is therefore essential that the final risk approval captures the thinking that went into the legal risk pillar to ensure accountability for decision makers.

Finding 9. NSIRA found that the scope of legal considerations within legal risk assessment is under-inclusive.

78. The importance of consistently memorializing legal risk was underscored when identifying non-Canadian criminal law risks. This includes risks arising from sources of civil liability, from foreign domestic law, and international law risks to Canada. The review revealed that it is not entirely clear to all parties which risk stakeholder is ultimately responsible for identifying and assessing these sorts of legal risks. For example, at separate briefings with GAC and the DOJ's National Security Litigation and Advisory Group (NSLAG), the former stated that their Legal Affairs Bureau was engaged in assessing international law, whereas the latter explained that their role is to identify all legal risks associated with CSIS operations.

79. There is some justification for both parties to assess international law risks, with NSLAG being legal adviser to CSIS on all areas of law with links to legal subject matter experts across the DOJ (including, for example, the Constitutional, Administrative, and International Law centre of expertise), while GAC Legal Affairs Bureau counsel support their Minister's duties in respect to the development and application of international law, including its application to Canada's external relations. [examples provided on risk assessments...] [redacted]

80. While CSIS may, as of 2019, use the justification framework to grant a source limited legal protection under Canadian law, this framework offers no protection under foreign domestic laws and is irrelevant when considering Canada's international law obligations. For example, if a source is granted protections under Canadian law through the justification framework for what would otherwise constitute offences that apply extraterritorially (e.g. terrorist financing, violations of sanctions), they can still face jeopardy under the legal regime where the operation is occurring. While acknowledging the attendant and practical difficulties, these types of risks need to be identified and considered in each relevant pillar (i.e. operation, legal, foreign policy and reputation risk).

Recommendation 4. NSIRA recommends that CSIS, in consultation with the Department of Justice and Global Affairs Canada, ensure that legal risk assessments are comprehensive and memorialized in writing.

Foreign Policy Pillar

Finding 10. NSIRA found that Global Affairs Canada and CSIS do not have a shared vision with respect to the role of Global Affairs Canada in the foreign policy risk assessment.

81. GAC and CSIS use two mechanisms to implement MD requirements for foreign policy risk assessments. The first is the [name of mechanism] which is used in the context of national security investigations, and foreign intelligence collection, while the [name of mechanism] is used for threat reduction measures. CSIS's centralized risk unit initiates the consultation process with GAC after identifying foreign policy issues, or as stipulated within the two mechanisms.

82. The review examined all of GAC's foreign policy risk assessments provided to CSIS for [redacted] (i.e. [redacted] total, of which [redacted] were high risk). In conducting this analysis, NSIRA took note of recent commentary by the National Security and Intelligence Committee of Parliamentarians Special Report on GAC, which observed that the Department has limited policies, procedures or internal committee structures to guide or oversee its provision of foreign policy risk assessments to CSIS.

83. Although non-compliance issues were not observed, CSIS and GAC had no agreed upon turnaround time for the latter's foreign policy risk assessments. NSIRA also observed that, on occasion, GAC requests to CSIS for additional assessment-related information were made only after CSIS's proposed operation had become an urgent priority. For example, CSIS had to follow up with GAC after waiting twenty-one days for a risk assessment. At this point, [redacted] which led CSIS to cite exigent circumstances under the consultation mechanism and proceed without the final submission. After CSIS executed the operation, GAC informed CSIS that the operation had carried a high risk.

84. In the broader analysis, the risk-consultation process between GAC and CSIS, while professional, is nonetheless at a crossroads. There is a concerted effort by CSIS to further restrain the flow of sensitive information to GAC to that which the Service believes is absolutely necessary for the foreign policy risk assessment.

According to CSIS, this restriction is to protect highly sensitive operational information from risk of unauthorized disclosure. In addition, CSIS wants to establish service standards for the timely production of these assessments. GAC believes it can meet any negotiated service standard so long as it is granted sufficient access to CSIS information. Project [redacted] could further complicate matters, [redacted] likely reducing GAC access to day-to-day operational information from CSIS. Any further limitations on insight into CSIS activities should be avoided, as this would generate an unacceptable accountability gap for the Minister of Foreign Affairs.

85. The importance of GAC having insight on certain CSIS activities was illustrated during [redacted] CSIS had not apprised GAC of this operation [redacted] This undermined the ability [redacted] to convey the impression that GAC had adequate knowledge of CSIS activities [redacted]

86. Managing Canada's foreign policy has become more complex in the ensuing years, particularly following recent diplomatic crises with China and India. As CSIS continues collection and threat reduction activities targeting foreign state actors, this will often engage the Minister of Foreign Affairs' accountability equities, and will likewise require consultation with GAC.

Recommendation 5. NSIRA recommends that any pending changes to CSIS's risk assessment process maintain a robust consultation and information sharing mechanism between Global Affairs Canada and CSIS.

Reputational Pillar

87. Following the [redacted] [operation] [redacted] PS believed that the [redacted] reputational risk rating assigned to the operation was flawed, and that the timing of the assessment failed to provide the Minister with sufficient warning. PS only learned from CSIS about the risk rating, rather than reviewing the actual assessment, exasperating PS's concerns. This prompted PS to question the sufficiency of CSIS's risk assessment process generally, and is the reason risk assessment became one of the central issues examined by NSIRA in this Ministerial referral.

88. Following an examination of the facts of this case, the risk assessment process was not the reason why the [redacted] operation was jeopardized. The risk

assessment process is not the sole trigger for ministerial engagement. All risk assessments contain elements of subjectivity and are open to challenge. Despite this inherent weakness, CSIS's [redacted] risk assessment followed the established process. CSIS and PS always retain the option of briefing the Minister, when appropriate, regardless of the risk rating.

89. While high-risk assessments must be briefed to the Minister prior to operational execution, and therefore may provide a limited window for earlier engagement, [redacted] More often than not, in cases that are not high risk, it comes down to sound judgement by senior leadership on when to engage the Minister.

90. Another factor to consider is that it is standard practice for CSIS to create risk assessments [redacted] [contextual information about risk process, and an example to emphasize issue...] [redacted] This was eight days after the Minister and PS had been informed by CSIS of the planned operation, and therefore, by this point everyone who needed to be aware had been informed.

Finding 11. NSIRA found that Public Safety is not adequately contributing to the preparation of reputational risk assessments.

91. NSIRA observed systemic challenges in the way that the reputational pillar of the risk assessment is organized. These challenges limit the degree to which the risk assessments facilitate ministerial control of CSIS. The 2019 MD on Accountability states that:

> Reputational risk is to be assessed, in consultation with Public Safety Canada, and include the potential for public controversy, as well as the risk of discrediting the Service or the Government of Canada.

92. First, as noted previously, there are no legal, policy or other documents that define 'consultation' outside of the context of the MD. PS has decided to interpret consult as meaning *after the fact*. Therefore, other than high risk operations where the Minister must be notified, the vast majority of reputational risk assessments are 'consulted' as part of information exchanged at meetings held under the PS/CSIS Cooperation Framework. These meetings occur on a quarterly basis, where CSIS provides examples of reputational risk assessments for specific operations. Given the fixed timing of these meetings, most of the operations discussed have either already commenced or are completed. PS may use this forum to provide strategic

guidance on reputational risk for future operations; however, CSIS told NSIRA that meaningful leadership in this respect is the exception.

93. This observation raises a second issue: "ownership" of the reputational risk assessment. All non-CSIS risk stakeholders – i.e. PS, GAC, DOJ – share the viewpoint that reputational risk is difficult to define and exists simultaneously within all of the risk pillars, and therefore, may not be assessed as comprehensively as warranted. The purpose of having separate risk pillars is to draw attention to specific considerations for approval authorities.

94. PS believes that providing strategic advice on reputational risk addresses the requirements of the MD. NSIRA, however, did not observe evidence of a comprehensive and systematic approach to assessing reputational risk. For example, PS informed NSIRA that CSIS had not consistently been performing reputational risk assessments for activities [redacted]

95. As this example suggests, in practice, reputational risk assessments are situated with CSIS. According to the Service, the risk program is run separately from operations, [redacted] administered by risk specialists who are solely responsible for this function. The approval authority for reputational risk is a senior manager who reports to the non-operational Deputy Director Policy and Strategic Partnerships. This group, being external to operations, is expected to bring a unique vantage point, being also responsible for Cabinet and Parliamentary Affairs, external communications and media relations, and is the principal interlocutor with PS on CSIS policy and governance matters. However, NSIRA believes that despite these internal CSIS guardrails, PS's decision to permit CSIS to make reputational risk assessments on its own is not without consequences.

96. The requirement in MD to undertake external consultation in assessing risk did not come about by accident. Rather, this accountability axiom emerged as a direct response to operational failures and recognition by Government that CSIS, however well intentioned, may not be best placed to consider all risk equities for the GC while carrying out operational activities. It is therefore essential to ensure that CSIS's risk assessment process will capture a diverse range of perspectives – and, in particular, a non-Service viewpoint in assessing reputational risk to the Government of Canada prior to operational execution.

97. Finally, it is instructive to compare the role played by PS with those of GAC and DOJ. When requested to do so, these departments each provide CSIS with an independent risk assessment. There is no use of proxy responsibility and after-the-fact consultation. Yet, PS provides no similar, independent input into the assessment, even on a topic (i.e. reputational risk) where it may be better positioned to consider reputational consequences for the Government as a whole.

Recommendation 6. NSIRA recommends that Public Safety and CSIS develop a more robust consultation mechanism for reputational risk assessment for CSIS operational activities, and that these assessments account for the risk of discrediting the Government of Canada.

4. Conclusion

98. The system of Ministerial accountability for CSIS is in need of serious attention. Building a stronger system of accountability now will help prepare for the inevitable [redacted] operations of the future, and reduce the likelihood of a repeat of the confusion and risk incurred [redacted]

99. Nevertheless, no amount of writing or wordsmithing of MDs, or improvements to risk processes, are a substitute for a culture of accountability. CSIS and PS must engage with each other with the common objective of ensuring that their shared Minister is seized with the information required to fulfill their ministerial responsibilities.

Annex A. [codename] – A Case Study

A1. [synopsis about what is contained within case study...]

Background

A2. [background information...]

CSIS did not declare this activity to their counterparts.

A3. [background information...]

A4. Key to operational activities on behalf of CSIS

[background information...]

[background information...]

A5. SIRC launched a review, which included an overview of the source operation The review contained findings and recommendations aimed at addressing a number of interrelated issues, including: legality of operations for sources participating in terrorist facilitation networks, ministerial direction, risk management, internal oversight, identity management, domestic and foreign partnerships, loss of operational environments and foreign strategic orientation. CSIS accepted all of SIRC's recommendations, and these improvements were subject to SIRC scrutiny in subsequent years.

A6. [background information...]

A7. [background information...]

A8. activities were a catalytic event for CSIS. The source was a direct result of CSIS failing to disclose the operation. This situation was further exacerbated when CSIS decided to

[background information...]

According to CSIS, the relationships has reportedly been on an

[redacted]

A9. [redacted] exposed limitations in Ministerial awareness of CSIS operations. Pursuant to the 2008 Ministerial Direction (MD) for Operations (i.e. the precursor for the 2015 MD), the Director needs to:

> Notify the Minister when there is a potential that a CSIS activity may have significant impact on Canadian interests, such as discrediting the Service or the Government of Canada or giving rise to public controversy.

A10. [redacted] This incident received executive level attention within CSIS about the appropriateness of [redacted] activities. Yet, CSIS did not inform the Minister of these events. In its [redacted] review, SIRC found that in order to comply with the 2008 MD, the CSIS Director should have notified the Minister [redacted]

A11. [redacted] SIRC also raised concerns about the legality of CSIS's activities. SIRC found that CSIS had failed to create a timely strategic plan that included legal advice, outlining clear parameters for [redacted] continued participation [redacted] At the time, CSIS viewed Crown immunity as a possible [redacted] abandoned this perspective in response to subsequent DOJ legal advice. The Federal Court discussed the difficult sequencing of legal advice on the Crown immunity question (and controversy over its application) in an unrelated decision concerning CSIS's candour in warrant applications.[3] Ultimately, the legal risks identified in the [redacted] operation provided motivation for the CSIS Act's justification framework, enacted into law by the National Security Act, 2017.

A12. [redacted]

---

[3] 2020 FC 616 at para 45 et seq. See also NSIRA Review 2021-18 on Federal Court.

[operational details...]

[operational details...]

[operational details...]

[operational details...]

[operational details...]

[operational details...]

[conclusion of operational details...]

Annex B. Role of Minister

The "Minister", for the purposes of the CSIS Act, is the Minister of Public Safety and Emergency Preparedness.[4] The Minister has several roles, including that in section 6(1): "The Director, *under the direction of the Minister*, has the control and management of the Service and all matters connected therewith."[5]

Development of the CSIS Act

B1. The nature of this ministerial direction was a focus of discussion prior to the enactment of the CSIS Act. The McDonald Commission of Inquiry, charged with scrutinizing wrong-doing by the RCMP Security Service in the 1970s, proposed the creation of what became CSIS. It discussed at length the degree of oversight the Minister should exercise over the proposed security service.

B2. It concluded that while the Minister was in no position to direct the "day-to-day operations of the agency any more than can the Minister of any other department", "there must be no fetters on the Minister's legal right to give such direction provided that such direction is consistent with the authority granted to the security intelligence agency under the Statute."[6]

B3. The Commission firmly rejected any distinction limiting the Minister to policy (as opposed to operational) direction, concluding that the boundary between the two concepts was unclear and uncertain. Thus, the Minister should be responsible for, among other things, "reviewing difficult operational decisions involving any questions concerning legality of methods or whether a target is within the statutory mandate". More generally, "where day-to-day operations raise significant policy questions, the Deputy Minister and [the security service head] must keep the Minister informed and seek his advice and direction."[7]

B4. The Commission rejected arguments that would put the intelligence service on a footing analogous to that of the police, who enjoy considerable operational independence. The risk that the intelligence service might be politicized by partisan

---

4 CSIS Act, section 2.

5 CSIS Act, subsection 6(1) (emphasis added).

6 McDonald Commission, Second Report, Volume 2, at 869.

7 Ibid at 869.

ministerial direction was to be mitigated, not by limiting ministerial oversight, but by a robust system of specialized review.

B5. The Commission underlined the importance of information flow enabling ministerial oversight. It recommended that, except in extraordinary circumstances, the intelligence service director should report through the Deputy Minister and not directly to the Minister. This, the Commission concluded, would "avoid the concentration of too much power in the hands of the" intelligence service director. Yet, while the Deputy Minister would be "the principal adviser of the Minister, including the area of responsibility covered by the" intelligence service, the service director (with the Deputy Minister's knowledge and consent) "should be reporting to the Minister on operational problems, and…policy proposals developed by the agency". The Deputy Minister must be equipped to "appraise for the Minister the quality of the reports produced by the agency so that the Minister can assess the agency's work", albeit with limits tied to source identity protection.[8]

B6. Following the McDonald Commission, the ultimate CSIS Act required two bills to enact, after members of Parliament and civil society condemned the original law project as too sweeping. Following this initial controversy, a special Senate committee proposed amendments to the original bill. Like the McDonald Committee, it too addressed the Minister's oversight role. This "Pitfield" Committee agreed that the Minister should give direction to CSIS. It also supported the codification of a role for the Deputy Minister in keeping the Minister informed of CSIS operations – something that would ensure that the CSIS Director "does not acquire the de facto status of deputy to the Ministers in matters of security".[9] It opposed a provision in the original bill that limited the Minister's ability to override the Director's decision on certain limited operational matters.

B7. The Committee wrote that this "override" limit would "insulate the Minister to too large a degree from operational matters. Affixing political responsibility for acts of the CSIS would be extremely difficult and thus effective control would be proportionately less likely".[10] The Committee shared the opinion of the McDonald Commission: the risk of partisan abuse by the Minister would be limited by effective specialized review of CSIS conduct. The Committee saw merit in the idea

---

8 Ibid at 870-871.

9 Special Committee of the Senate of the Canadian Security Intelligence Service, *Delicate Balance: A Security Intelligence Service in a Democratic Society* (November 1983) at 26.

10 Ibid at 27.

that "ministerial interventions should have to be formally submitted, in writing, to the Director and also transmitted" to the review body.[11] It also concluded that "[i]n any event, the danger of political abuse is far outweighed by the need for effective control and responsibility".[12]

B8. While the Minister should rarely intervene in operations, there should be no legal fetter on their doing so. Instead, CSIS "should be an 'open book' to the Minister, who will consequently have full political responsibility for matters about which [the Minister] can be expected to have knowledge."[13]

CSIS Act

B9. The final CSIS Act codified a specific oversight role for the Minister in several areas, including of an operational nature.[14] Amendments in 2015 and 2019 expanded this list.[15] As noted, section 6 subjected the Director's control of CSIS to the direction of the Minister. This provision includes no "override" of the sort limiting ministerial direction found in the original (rejected) CSIS bill. It contains no distinction between policy and operations.[16]

---

11 Ibid at 27 and 28.

12 Ibid at 27.

13 Ibid at 28.

14 CSIS Act, section 3 (creation of regional offices); section 13 (arrangements for security assessments with other jurisdictions); section 17 (arrangements with police forces or intelligence services); subsections 21 and 22 (approval of a warrant application and renewal).

15 CSIS Act, section 11.03 (classes of Canadian datasets); section 11.07 (retention of foreign datasets); section 20.1 (classes of offences under the justification regime); subsection 11.01 et seq; 20.1 (designation of employees to perform certain functions under the dataset and justification regimes); subsections 21.1 and 22.1 (approval of threat reduction warrant application and renewal).

16 Section 6(2) does provide that the Minister's directions to CSIS may be in writing, and that a copy be given ("forthwith after it is issued") to the National Security and Intelligence Review Agency. The provision has not, however, precluded oral directions, a phenomenon that the House of Commons special committee on the CSIS Act criticized in 1990, because it made review more difficult. House of Commons Special Committee on the Review of the Canadian Security Intelligence Service At and the Security Offences Act, *In Flux But Not in Crisis* (September 1990) at 92. See also House of Commons, Standing Committee on Justice and Legal Affairs, vol 2 no 21-32, (7-6-1984) at 38:26 and 38:27. Under its own Act, the Review Agency "must review the implementation of significant aspect of every new or modified ministerial direction". NSIRA Act, section 8(2.1).

B10. In terms of information flow to the Minister, section 6 does not include specific instructions that the Director keep the Minister informed of CSIS operations. Parliamentarians rejected a proposed amendment to that effect in clause-by-clause in the House of Commons in 1984. However, this rejection came after the Minister explained that this information obligation was already implicit in established duties on officials.[17]

B11. The Act does specify that the CSIS Director must consult with the Deputy Minister on the general operational policies of CSIS, warrant applications, or any matter for which consultation is required by ministerial direction.[18]

Later Parliamentary Scrutiny

B12. In reviewing the CSIS Act in 1990, the House of Commons special committee on the CSIS Act concluded that section 6 "places the [Minister] firmly in the driver's seat by making the Director's control and management of the Service subject to written ministerial directions".[19] By then, ministerial direction under section 6 had reached operations. For instance, in 1988, the Minister directed that any investigation of subversion (paragraph d of the definition of "threats to the security of Canada") beyond open source requires approval of the Minister.[20]

---

17 House of Commons, Standing Committee on Justice and Legal Affairs, vol 2 no 21-32, (7-6-1984) at 38:27.

18 CSIS Act, section 7

19 House of Commons Special Committee on the Review of the Canadian Security Intelligence Service At and the Security Offences Act, *In Flux But Not in Crisis* (September 1990) at 92.

20 House of Commons Special Committee on the Review of the Canadian Security Intelligence Service At and the Security Offences Act, *In Flux But Not in Crisis* (September 1990) at 24.

ANNEX C. Findings and Recommendations

Accountability and Consequences for Halting [codename] *Operation*

Finding 1: NSIRA found that a decision was made to halt an active CSIS operation overseas that was not made by the CSIS Director under section 6(1) of the CSIS Act, and for which there is no written record of a direction coming from the Minister of Public Safety under sections 6(1) or 6(2) of the CSIS Act.

Recommendation 1: NSIRA Recommends that whenever there is a decision affecting an active CSIS operation, which is not made by the Director of CSIS or their delegates, it must come as a direction from the Minister of Public Safety under section 6(1) of the CSIS Act and should be accompanied by a written record in keeping with section 6(2).

Finding 2: NSIRA found that [*] **halted an active operation, creating unnecessary danger for the CSIS team** [redacted] **and caused harm to Canada's international reputation.**

Responsibility for Briefing the Minister [about codename]

Finding 3: NSIRA found that Public Safety and CSIS failed in their responsibility to provide timely and accurate information to the Minister of Public Safety about [redacted] **human source** [redacted] **operation.**

Public Safety's Role in Relation to CSIS

Finding 4: NSIRA found that Public Safety willingly remains dependent on CSIS to identify and receive relevant information, which inhibits Public Safety's ability to prepare independent advice to the Minister about the activities and operations of CSIS.

Recommendation 2: NSIRA recommends that the Minister of Public Safety take action to ensure that the Deputy Minister obtains any information required to fulfill their responsibility to provide independent advice to the Minister about the activities and operations of CSIS.

Ministerial Direction to CSIS

Finding 5: NSIRA found that multiple Ministerial Directions to CSIS are subject to inconsistent and contradictory interpretation by those responsible for their implementation.

Finding 6: NSIRA found that when preparing Ministerial Directions to CSIS, Public Safety insufficiently consulted with Global Affairs Canada and CSIS.

Recommendation 3: NSIRA recommends that the Minister of Public Safety consolidate ministerial directions into clear, concise and harmonized instruments that are derived from meaningful consultation among those responsible for their implementation.

CSIS's Risk Assessment Process

Finding 7: NSIRA found that CSIS's risk assessment process has evolved to become the central mechanism for planning operations and managing associated risks, and, while it is generally effective, it lacks clear guidance to employees on when risk should be reassessed as operations evolve.

Legal Pillar

Finding 8: NSIRA found that legal advice is often absent from the final risk assessment record for CSIS operations.

Finding 9: NSIRA found that the scope of legal considerations within legal risk assessment is under-inclusive.

Recommendation 4: NSIRA recommends that CSIS, in consultation with the Department of Justice and Global Affairs Canada, ensure that legal risk assessments are comprehensive and memorialized in writing.

Foreign Policy Pillar

Finding 10: NSIRA found that Global Affairs Canada and CSIS do not have a shared vision with respect to the role of Global Affairs Canada in the foreign policy risk assessment.

Recommendation 5: NSIRA recommends that any pending changes to CSIS's risk assessment process maintain a robust consultation and information sharing mechanism between Global Affairs Canada and CSIS.

Reputational Pillar

Finding 11: NSIRA found that Public Safety is not adequately contributing to the preparation of reputational risk assessments.

Recommendation 6: NSIRA recommends that Public Safety and CSIS develop a more robust consultation mechanism for reputational risk assessment for CSIS operational activities, and that these assessments account for the risk of discrediting the Government of Canada.