Overview of Ministerial Oversight & Accountability for the Canadian Security Intelligence Service (CSIS)

by

Olivia Tubman
B.A., Graceland University, 2015

A Master's Project Submitted in Partial Fulfillment of the Requirements for the Degree of

MASTER OF PUBLIC ADMINISTRATION

in the School of Public Administration

© Olivia Tubman, 2019
University of Victoria

All rights reserved. This thesis may not be reproduced in whole or in part, by photocopy or other means, without the permission of the author.

Overview of Ministerial Oversight & Accountability for the Canadian Security Intelligence Service (CSIS)

Olivia Tubman, MPA Candidate
School of Public Administration
University of Victoria
November 29, 2019

Client:	Steve Tharakan, Manager National Security Policy Directorate Public Safety Canada
Supervisor:	Dr. Evert Lindquist, Professor School of Public Administration University of Victoria
Second Reader:	Dr. Emmanuel Brunet-Jailly, Professor School of Public Administration University of Victoria
Chair:	Dr. Astrid Perez Pinan, Assistant Professor School of Public Administration University of Victoria

ACKNOWLEDGEMENTS

I wish to extend my thanks and immense gratitude to the following individuals:

To Dr. Evert Lindquist, for your support as my supervisor, and your simultaneously thoughtful and thought-provoking feedback and advice. It only served to make this a better project and by extension make me a more critical thinker.

To my colleagues, for your constant encouragement and support, and for always being willing to lend a listening ear.

To Steve Tharakan, for not only being willing to represent NSPD when I undertook this project, but for also your unwavering support, patience and belief in me throughout this entire process. Thank you for bringing valuable perspective for those moments when I inevitably got lost in the details.

And finally, to my family and friends, for your tireless support and confidence in my ability to be successful at whatever I put my mind to - even when it means moving across Canada to do it. Whether you're near or far, or an old friend or a new one, it is abundantly clear that I would not have made it to this point without each and every one of you in my corner. Thank you all for everything.

EXECUTIVE SUMMARY

The role of Ministerial oversight of the Canadian Security Intelligence Service (CSIS) within the national security accountability framework has largely been left unchanged since CSIS was first established in 1984. However, both the role of the Minister for CSIS and the scope of activities and functions CSIS has been mandated to perform have significantly expanded in the succeeding decades. This expansion of powers and authorities has not always coincided with changes to the accountability framework; however, with the passing of the *National Security Act, 2017* on June 21, 2019, the framework has undergone significant change to further increase accountability for CSIS and the broader national security and intelligence (NSI) community as a whole. These changes are largely the resulting culmination of several different factors, including an evolving threat environment, organizational changes over several decades, and an internal and external push for increased transparency within the NSI community.

This paper will conduct a comparative historical analysis of the accountability framework for CSIS between 1984 and 2019, looking specifically at both how the framework has evolved over time and how the process for accountability has changed since it was first established. In order to do this, the paper will examine possible reasons or circumstances for why these changes took place and will look at how this framework compares to two of Canada's closest international allies. The analysis will also look ahead to changes being implemented at the time of writing, following Royal Assent of the *National Security Act, 2017*.

All information contained in this paper was derived exclusively from open source information and is unclassified. Sources consist primarily of published journal articles, books, and public government documents, and is supplemented by interviews with current government officials who have worked in departments or agencies relevant to the CSIS accountability framework and the process for Ministerial oversight of CSIS.

Project Objectives

The primary objective of this project is to improve understanding of the role of the responsible Minister, including the parameters regarding oversight, in the CSIS accountability framework in past, present and future contexts. This involves the following: the completion of a comparative historical analysis which details how the national security accountability framework for CSIS has evolved since the McDonald Commission in 1981 and the implications this has had for the role of Ministerial oversight; and the development of an analytical framework that identifies key elements of the role of Ministerial oversight and accountability for CSIS, including responsible entities and organizational structure of the framework.

Research Question: Following the final McDonald Commission report in 1981, and the consequent establishment of CSIS in 1984, how has the evolution of the national security accountability framework impacted the role of Ministerial oversight of CSIS?

> **Sub-Research Question A:** To what extent will future changes to legislation of CSIS through Bill C-59 impact the role of Ministerial oversight for CSIS?

Sub-Research Question B: Given the proposed changes, what are possible implications to Ministerial oversight of CSIS and the national security accountability framework?

Sub-Research Question C: What can be learned from past changes to the national security accountability framework and Ministerial oversight of CSIS, and how these lessons apply to the proposed new framework?

Methodology

The objective of this project is to contribute a comparative historical analysis and analytical framework to Public Safety Canada, with the aim of improving understanding of the role of the responsible Minister, including identifying the parameters regarding Ministerial oversight and accountability. This will be examined alongside past and current environmental contexts and look at how these contexts may have impacted the evolution of the framework.

In order to meet this objective, the following two-step process has been utilized:

1. First, the completion of comparative analysis of how the national security accountability framework for CSIS has evolved since the McDonald Commission and the implications this has had for the role of Ministerial oversight; and,

2. Second, interviewing current government employees to further identify key elements of the role of Ministerial oversight and accountability for CSIS, including functions, responsibilities, and organizational structure.

Key Results

The key findings from the report are as follows:

1. The significance of conducting Ministerial oversight of CSIS was a key component in the development of the accountability framework for CSIS, and has endured since CSIS was first established in 1984. However, Ministerial oversight has encountered challenges since the early 2000's:

    a. First, when significant organizational changes to the Ministerial portfolio took place, expanding the number of organizations for which the Minister was responsible for; and,

    b. Second, when CSIS was provided with an increasing number of powers and authorities to adapt to the changing threat environment that were not simultaneously met with additional supports for the responsible Minister or the other entities within the accountability framework.

    With the changes coming into force following the passage of the *National Security Act, 2017*, Ministerial oversight of CSIS will not experience significant changes; however, the

remainder of the framework has been expanded to provide additional mechanisms for review and oversight of CSIS, and could lead to changes to Ministerial oversight.

2. Transparency in the NSI-context is primarily about finding transparency mechanisms that both balances the need for helping Canadians understand the necessity of having an agency like CSIS to protect the country from threats without revealing too much about how they do so and assures Canadians that the rights and freedoms Canadians are entitled to are only intruded upon in a lawful way and when exigent circumstances arise. When the accountability framework was first established in 1984, it was one of the first in the world where both the agency and the accountability framework was publicly acknowledged by the country's government. In many ways, this model was considered by Canadians and international experts as an ideal example for NSI agencies around the world.

   Thirty-five years after the establishment of CSIS, the activities conducted by CSIS and other NSI agencies have received a steadily increasing amount of public attention and scrutiny. This has been in part because of the public's knowledge of certain events (such as the Edward Snowden disclosures) and because of an increasing push for improved transparency, something that has occurred both within and outside of government. This has presented a challenge unique to the realm of NSI agencies. An increase in visibility has led to more exposure for CSIS and much of the Canadian NSI Community, which presents a potential challenge for CSIS in protecting Canadians from security threats if information about certain activities is revealed.

3. The increased amount of scrutiny on CSIS and the NSI Community, most recently demonstrated quite prominently by the findings of the public consultations held by the government in 2016 with Canadians and subject matter experts in which accountability and interest in CSIS and NSI activities were clearly expressed by many participants, has led to a series of reactive changes to the accountability framework. This includes the creation of new review and oversight entities for both CSIS and the broader NSI Community, as well as specific amendments to activities and authorities granted to CSIS. However, in order for review and oversight to be truly effective for CSIS, an understanding of past, present and potential future threat environments is required by CSIS and those entities responsible for holding the agency accountable.

4. Beyond what has already been changed with the passage of the *National Security Act, 2017*, there remain certain opportunities for enhancing or refining review and oversight of CSIS. The three policy options presented in this paper include enhancing the role for the Deputy Minister of Public Safety Canada in supporting Ministerial oversight of CSIS, decreasing the size of the Minister's portfolio, and requiring the National Security and Intelligence Committee of Parliamentarians (NSICOP) to conduct regular parliamentary review of the CSIS accountability framework.

TABLE OF CONTENTS

1. INTRODUCTION

Established in 1984, CSIS has had accountability as an integral part of its governing framework from the beginning. The accountability framework relies on internal and external review and oversight mechanisms for the agency and external stakeholders, including the public (Wark, 2015). This multi-layered system of review and oversight was structured to ensure that Canada's first NSI agency meets its legislated mandate. Review and oversight were considered as vital, non-negotiable factors when developing its statutory framework.

Prior to establishing CSIS, oversight of NSI agencies in Canada was not common practice (Farson, 2000, p. 226). With the creation of CSIS, significant changes were made to the NSI community in Canada, including setting a precedent of accountability for other agencies. The 1981 Royal Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (the McDonald Commission) not only called for a new agency as the threat environment continued to evolve through the last decade of the Cold War, but also indicated that it would need strong accountability and oversight mechanisms. Following the establishment of CSIS in 1984, the main entities responsible for conducting review and oversight of CSIS included the Security Intelligence Review Committee (SIRC), the Inspector General, the Solicitor General of Canada (the responsible Cabinet Minister for CSIS), and the Federal Court of Canada (FC). They were intended to complement each other in order to avoid a duplication of responsibilities and to ensure that the most comprehensive structure for accountability was in place for CSIS.

Since 1984, CSIS has operated with virtually the same accountability framework. The changes to the framework that occurred in the succeeding decades were primarily in response to the evolving national security threat environment. These included organizational changes for government departments and agencies, leading to shrinking or expanding of Ministerial roles and responsibilities within the Canada's NSI community; further commissions of inquiry into the actions taken by members of the Canadian NSI community; and changes to legislation that altered the scope of powers and activities for CSIS. The fundamental premise and structure of the accountability framework has remained mostly unaltered for thirty-five years. The best example of this is Ministerial oversight, which has been an enduring component of the accountability framework and has experienced minimal change in how the Minister conducts oversight for CSIS. However, the overall policy portfolio of the Minister responsible for oversight of CSIS has expanded significantly since 1984, raising concerns about a lack of additional means to accompany the increased responsibility. In recent years these concerns have surfaced with more frequency from experts and external stakeholders concerned about the ability of the Minister to conduct effective oversight and hold CSIS accountable.

Examining past changes to CSIS's accountability framework has become even more important given the recent passage of Bill C-59, *An Act respecting national security matters* (the *National Security Act, 2017*) in 2019. Through a combination of new and amended legislation, the *National Security Act, 2017* promises to significantly alter the accountability mechanisms for CSIS, particularly in relation to the entities responsible for conducting oversight and review. This includes Ministerial oversight. The primary objective of this project is to improve understanding of the Minister's role and the parameters of the responsible Minister in past,

present and future contexts. The client for this paper, the National Security Policy Directorate at Public Safety Canada, has requested the following:

That the primary research question guiding this report be:

> *Following the McDonald Commission reports in 1979 and 1981, and the consequent establishment of CSIS in 1984, how has the evolution of the national security accountability framework impacted the role of Ministerial oversight of CSIS?*

Three related subsidiary research questions are as follows:

A. To what extent will future changes to legislation of CSIS through the *National Security Act* impact the role of Ministerial oversight for CSIS?

B. Given the changes coming into force, what are possible implications to Ministerial oversight of CSIS and the national security accountability framework?

C. What can be learned from past changes to the national security accountability framework and Ministerial oversight of CSIS, and how these lessons apply to the new framework?

To inform answers to these questions, the client has requested the following methods are used:

1. Comparative research and analysis of how the national security accountability framework for CSIS has evolved since the McDonald Commission and the implications this has had for the role of Ministerial oversight. This includes examining how Ministerial oversight and reviews through the accountability framework have contributed to any organizational and institutional changes within CSIS and, if appropriate, other departments with an NSI-nexus mandate (such as Public Safety Canada), and examine how these review mechanisms coexist and how they react to changes in the national security environment.
2. Developing analytic frameworks that identify key elements of the role of Ministerial oversight and accountability regime for CSIS, including functions, responsibilities, and organizational structure. The goal is for Public Safety Canada to use this framework to support the Minister in carrying out their responsibilities and inform policy development by furthering historical understanding of the organizational structure of accountability and Ministerial oversight and the implications of previous changes.

This report has 11 sections. Following the introduction, Section 2 provides more detailed background on CSIS, Ministerial oversight and accountability. Section 3 delves further in the methodology and methods used to undertake the research for this report. Section 4 reviews the accountability and organizational frameworks for the CSIS at three crucial periods over the last thirty-five years. Section 5 outlines two international models for accountability of NSI agencies. Section 6 examines the evolution of the threat environment in Canada. Section 7 discusses several of the challenges to ensuring accountability of CSIS. Section 8 reviews the findings and provides an analysis. Lastly, Sections 9 and 10 presents options and a recommendation for the future of the accountability and Ministerial oversight of CSIS, before concluding the paper in Section 11.

Additional supporting information, including visuals, will be located in the Appendix.

2. BACKGROUND

This report has been prepared for the National Security Policy Directorate, housed within Public Safety Canada. The following section will first provide key definitions, and then outline both the historical context for the creation of CSIS and the foundations of the accountability framework.

Key Definitions

The following definitions will be used when outlining the key roles and responsibilities of CSIS and others comprising the national security accountability framework, as well as Ministerial oversight. These definitions will inform the context and findings in this report. Additionally, it must be noted that these definitions are directly applicable to the Canadian NSI accountability context. In the official literature for other countries that are considered to be traditional allies of Canada in the NSI policy area, there are some key differences to how features of the accountability framework are defined. Oversight is most prominent example of this. In contrast, for certain key terms such as "national security", there are no official definitions produced in the Canadian context. As a result, these definitions were determined by analyzing literature, and by inquiries with individuals familiar with the Canadian NSI context.

National Security. There is no single definition of national security in Canada. One of the reasons for this is that the national security context is frequently evolving and consequently requires national security to be understood in the context of the time in which it is being referred to. In 1981, the McDonald Commission defined national security as the actions undertaken to preserve Canada and the Canadian government democratic processes from violent internal and external attacks (in Rankin, 1986, p. 250). This definition continues to provide, in broad strokes, the foundation of Canada's national security area today and provides the basis for the core mandate for Canada's NSI agencies and the threats they are protecting against.

Accountability. Brenton (2015) defines accountability as the "relationship between an account-holder (or principal) and accounter (agent), where the accounter has an obligation to provide an account to the account holder and is subject to external scrutiny from the account-holder" (p. 468). The concept of an entity being obligated to provide information on their activities to someone (or something) else outside of the entity under scrutiny, and for that other entity to be able to conduct review or oversight of the entity conducting activities, is historically a recent phenom for NSI communities around the world, including in Canada. In Canada, accountability not only helps detect and identify abuses of the powers and authorities granted to NSI agencies but contributes to developing a culture internally that does not support these transgressions (Wark, 2015, p. 2). In the Canadian national security framework, the accounter is the appropriate Minister, who is obligated to answer for the actions of their department or portfolio, and the account-holder is the Parliament of Canada and the public who elected these officials (including the responsible Cabinet Minister) to represent them in Parliament. Determining accountability can be determined after the fact, as part of an official review by the appropriate review body, or as part of a "process by which officials and organizations provide explanations and justifications for their conduct" (Forcese & Roach, 2015, p. 364).

Oversight. Oversight is the first component of the CSIS accountability framework. Depending on where in the world it is used, the definition for oversight in the NSI government context differs. In Canada, oversight only occurs when the entity responsible for oversight makes a determination prior to an activity actually occurring, not after the activity has already occurred (SECU Evidence, April 17, 2018). The latter process is considered to be review, as nothing can prevent the action from occurring. This process means that oversight must be directly integrated into the decision-making process; in this case, the stage where authorization or approval of an activity is required. The actual process of oversight, in the context of the CSIS accountability framework, is best defined in the SIRC Annual Report of 1985-86, where it is described as being the process of real-time "monitoring and evaluation… [of] security intelligence operations" (p. 3). Further, oversight is generally applied to matters involving "operational command and control strategy" (Forcese, Roach & Sherriff, 2015, p.1) and often requires a decision to be made. Engaging in oversight also indicates that all necessary entities are properly "informed and [have] powers of co-ordination and, where appropriate, control and direction that a review body will not have" (Commission of Inquiry into Actions of Canadian Officials in Relation to Maher Arar [Maher Arar Inquiry], 2006, p. 328). This has been further supported by decisions made by the FC.

Review. This is a second component of ensuring accountability for NSI departments and agencies; but, unlike oversight, which is conducted before an activity takes place, review cannot occur until after-the-fact. The Canadian definition of review is notably distinct from oversight, primarily because of the timing. Known as an ex post facto process, review cannot occur until after an activity has already happened. In the NSI context, this is particularly important, as this timing helps to avoid any possible interference in the carrying out of activities to protect the security of the nation and its citizens. However, there are other countries whom Canada is allied with that describe oversight and review as terms that are, for the most part, interchangeable and not distinct. In Canada, review is considered to be an integral component of an effective accountability framework, and not as something separate (Farson, 2000, p. 231). Review can be conducted through internal processes, or by an independent or third-party process. SIRC, formerly the primary entity responsible for conducting review of CSIS, described their review role as allowing them to "make a full assessment of CSIS's past performance without being compromised by an involvement in its immediate, day-to-day operational decisions and activities" (SIRC, 2014, p. 12).

Ministerial Accountability. Ministers in the Queen's Privy Council of Canada (more commonly referred to as the Cabinet) are both responsible and accountable to Parliament, and by extension, as an elected representative to Parliament, accountable to the public for how their powers are exercised in running of their individual departments and agencies (Parliament of Canada, n.d.; Office of the Prime Minister, 2015, section I.3). This is an institutional reality that spans the entirety of government, not just those departments and agencies within the NSI community. In Canada, Cabinet Ministers are held accountable through several different mechanisms: they can testify to Parliamentary committees, as well as the House of Commons; they can act to resolve situations in the departments or agencies for which they are responsible; or, if they cannot resolve the issue, the Minister can resign (Lagasse, 2010, p. 11). However, the onus falls solely on the responsible Minister to act to remedy identified issues, as they are the only ones who are accountable and responsible for the actions of their respective departments and agencies

(Lagasse, 2010, p. 11). Further to their role as appointed Cabinet Ministers, Ministers have a "clear ministerial accountability to Parliament… [which] is fundamental to responsible government" and is the ultimate demonstration of their accountability to the public (Office of the Prime Minister, 2015, s. III).

Ministerial Responsibility. Ministerial responsibility supports Ministerial accountability, in that it is the "legal, political and administrative responsibility" of a given Minister to be answerable for the actions of their respective department and agencies (Farson, 2000, p. 230). The foundations of the Canadian parliamentary system are based on the concept of responsible government, considered by the McDonald Commission to be an "essential requirement" of democracy (McDonald, 1981, p. 408). In order to ensure the continuance of responsible government with the creation of a domestic national security agency, the Minister would be expected to know about any policy or legal issues arising from any operational practices or policies of the agency (McDonald, 1981, p. 408).

Ministerial Oversight. Ministerial oversight is a specific component of the oversight process, in which the responsible Minister of a department or agency conducts oversight of proposed activities for the particular department or agency. It also acts as an accountability mechanism for the Minister to ensure the department or agency is performing within their mandate and can be effectively held accountable by the Minister. In Canada, the degree of oversight conducted by a Minister is dependent "on the nature of the [government] organization and the Minister's role" (Office of the Prime Minister, 2015, s. I.3). The Minister, in the case of CSIS, is the Minister of Public Safety and Emergency Preparedness (the Minister), formerly the Solicitor General of Canada. In the accountability framework for national security in Canada, Ministerial oversight has a central role for ensuring the activities conducted by departments and agencies in the Minister's portfolio are done so lawfully and in compliance with their legislated mandates.

Compliance. This is the ultimate objective and outcome for an NSI accountability framework. Compliance is something that underlies both review and oversight, as it establishes a set of criteria against which oversight and review bodies use to monitor and evaluate the lawfulness of an organization's activities (Forcese, Roach, & Sherriff, 2015, p. 8). Compliance in the review context is a process where the review entity identifies whether an NSI agency has fully complied with their legislative mandate. As a result, reviews in government are focused primarily on legal compliance (Farson, 2000, p. 230). Legal compliance is a significant component of review and oversight for the accountability of NSI agencies. In the past, there has been other compliance mechanisms for CSIS, including certification (such as by the former Inspector General). These certifications look at the scope of activities and whether they were, in the eyes of the review entity, necessary and reasonable in the set of circumstances.

Origins of a Domestic National Security Intelligence Service in Canada

The use of NSI agencies in Canada became increasingly imperative following the conclusion of the Second World War, during which the necessity and importance of intelligence activities was demonstrated by the Allied nations (Farson, 2000, p. 226). However, intelligence and other national security-related activities conducted in Canada go as far back as pre-Confederation, and were largely completed by the RCMP (Rutan, 1985, pp. 19-20). Following the Second World

War, the Special Branch of the RCMP, a division that was separated from the day-to-day operations of the RCMP, was established; the Special Branch eventually became the Directorate of Security and Intelligence in 1956, before finally transitioning to the RCMP Security Service (Rutan, 1985, pp. 20-21).

Immediately after the Second World War, the Canadian government was primarily focused on establishing an agency or agencies with NSI capabilities. There was little consideration or support for implementing review or oversight mechanisms for intelligence agencies, particularly because there was general belief that only those involved in intelligence operations could have access to intelligence (Farson, 2000, p. 226). This general consensus regarding intelligence agencies was shared by most Western democracies and would only begin to shift during the 1970s following several events that drew increased attention to the need for establishing accountability mechanisms for NSI agencies. The USA, for example, was among the first Western democracies to reform the accountability structures for their NSI agencies, following both the Watergate scandal and damning reports about the breadth of abuses being conducted by the Central Intelligence Agency (CIA) (Farson, 2000, p. 226).

Similar to the USA, Canadian NSI agencies were not immune to scandal during this time. Despite inquiries in the 1960s and 1970s into the activities conducted by the RCMP Security Service, including a Royal Commission of Inquiry in 1968, the idea of increasing oversight of Canadian intelligence agencies and their operations remained unpopular both publicly and within government until the early 1980s. This was likely due to an understanding that if intelligence activities were discussed more publicly it would expose the country to possible danger. There was also the belief that, because intelligence agencies were expected to function separately from government departments, they should not be subject to the same degree of oversight (Farson, 2000, pp. 227-228). The scandals that emerged in the 1970s led to another Royal Commission of Inquiry into RCMP activities instigated by the government, and this reporting became the first concrete step towards reforming the NSI community in Canada. The inquiry, known as the McDonald Commission, led to the disbanding of the RCMP Security Service and the creation of CSIS as Canada's first NSI agency with a formalized, public accountability framework (Whitaker, 1996, p. 280).

The McDonald Commission was not the first government inquiry to recommend reforming the RCMP Security Service. In 1968, the Royal Commission on Security (known as the Mackenzie Commission) privately provided the government with recommendations for the RCMP. They went as far as recommending that the government create a civilian-led intelligence agency separate from the RCMP (Government of Canada, 1983, para 6; McDonald, 1981, p. 671). At the time, the RCMP expressed several concerns related to disassociating security and intelligence activities from the federal law-enforcement body, including the RCMP already having well-established intelligence collection infrastructure and connections in the national security community with the RCMP Security Service, and broader security concerns related to the international nations like the Soviet Union capitalizing on the vulnerabilities of a civilian security service (McDonald, 1981, pp. 671-672). These reasons were largely accepted by the government and the recommendation was rejected as not a viable option for any intelligence service in Canada at the time (Rutan, 1985, p. 18).

However, less than a decade after the Mackenzie Commission, it was revealed that officers in the RCMP Security Service had used unsanctioned activities while performing their duties (Rutan, 1985, p. 17). These public revelations led to the government establishing the McDonald Commission in 1977, which was asked to identify if and what illicit activities took place, and to make recommendations "regarding the reorganization and restructuring of the entire security intelligence apparatus" (Rutan, 1985, pp. 17-18) in Canada. The McDonald Commission provided recommendations in 1981, and for a second time, it was recommended that Canada create a domestic intelligence service separate from the RCMP, with a mandate to investigate matters specific to national security. Further, the domestic intelligence service should be civilian-based and would not have the same law enforcement capabilities or mandate of the RCMP. The McDonald Commission firmly recommended that the new intelligence agency would need to be subject to a multifaceted and layered structure of control and review mechanisms to ensure it was effectively held accountable (Government of Canada, 1983, para. 1).

Flowing from these recommendations, the accountability framework for a new intelligence agency would need to be designed to utilize both oversight and review in the most effective manner possible to ensure the new agency would be held accountable for all of its activities, both before they occur and after. Oversight of the new security intelligence agency should occur across multiple areas of the government structure (including both the executive and judicial branches of government), a process designed to ensure that the tools of the new agency would be utilized effectively, and in compliance with the agency's legal mandate (Forcese & Roach, 2015, p. 362). Similarly, the proposed review mechanisms within the accountability framework should directly address how the new agency's activities could be monitored after the fact by an external, independent review body, which would be directly accountable to the government and the public through an annual reporting mandate. Unlike the RCMP Security Service, it was recommended that the new agency should have its functions clearly delineated through either "an Act of Parliament, Order-in-Council or administrative directive" (From McDonald Commission, found in Weller, p. 422), making public the NSI agency and its respective accountability framework.

Establishing an effective structure for review and oversight of the new agency was a major component of the new accountability framework. This concept was supported by legislation first proposed in 1983, the first iteration of what would become the CSIS Act. The proposed bill was examined more thoroughly in a study commissioned by the Special Committee of the Senate on the CSIS, often referred to as the Pitfield Report for the Chair of the committee which produced the study. This Special Committee was mandated to review the legislation after it was tabled in the House of Commons and sent to the Senate for review.

The Special Committee published the Pitfield Report, entitled *Delicate Balance: A Security Intelligence Service in a Democratic Society: Report of the Special Committee of the Senate on the Canadian Security Intelligence Service*. It focused on the degree of accountability needed for such an agency and recommended a series of changes to the Bill to increase accountability and oversight for the proposed agency. Among the suggestions included a role for the judiciary in providing oversight of any intrusive investigative activities by the proposed security service (Government of Canada, 1983, para. 100). Additionally, the report stated that the Minister responsible for the agency, not the Director, should maintain "full political responsibility for matters about which he reasonably can be expected to have knowledge" (Government of Canada,

1983, para 83). This reference to balancing both political and executive responsibility became a central component for the accountability of NSI agencies, as it not only echoes the executive responsibility all Cabinet Ministers hold when they take their oath of office but also references the accountability to the public as elected members of Parliament and the responsibility that entails. A final, yet crucial, element of the accountability framework recommended by the Pitfield Report was that the proposed review entity, SIRC, table an annual report to Parliament and share an unclassified version with the public (Government of Canada, 1983, para. 97).

Following the Pitfield Report, a new Bill was proposed that incorporated some of the recommendations from the McDonald Commission and the Special Committee. This Bill, known now as the *Canadian Security Intelligence Service Act* (the CSIS Act), received Royal Assent in the early summer of 1984, establishing Canada's first civilian NSI agency.

The Canadian Security Intelligence Service

The coming into force of the CSIS Act and the subsequent creation of CSIS in July 1984 allowed the government to clearly identify the role of an intelligence agency in the Canadian NSI framework and establish parameters within which the agency would operate (Rutan, 1985, p. 21). CSIS's accountability framework would operate within what the McDonald Commission called a democratic framework, where the parameters for the powers and activities of the new agency were established under the rule of Canadian law (Rutan, 1985, p. 19; McDonald, 1981, p. 47). The accountability framework introduced in 1984 incorporated complementary review and oversight mechanisms for CSIS, as well as a detailed statutory mandate, roles for Ministerial and judicial oversight, and a process for legislated review by a parliamentary committee five years after Royal Assent (Whitaker, 1992, p. 53). Additionally, the level of oversight for CSIS is more significant than other departments or agencies, as the Minister had (and continues to have) specific legislated responsibilities to be made aware of and, if appropriate, authorize specific activities before they occur (e.g. warrant applications) (CSIS Act, s. 21).

CSIS was given a mandate to investigate activities suspected to constitute threats to the security of Canada, as well as to take measures to reduce these threats where it was legally allowed or directed by the Minister (Government of Canada, 1a). CSIS was, and continues to be, authorized to collect and analyze threat-related information, safeguard confidential Government of Canada information, and prevent non-Canadians from entering Canada, receiving permanent resident status, or receiving citizenship, if these individuals pose a security concern (Government of Canada, 1a). To accomplish this mandate, CSIS is responsible for protecting sources and its methods, which has consequently led to CSIS keeping much of its work secret from the public as a matter of national security (SIRC Annual Report, 94-95, p. vii). However, some information is made available to the public by SIRC annual reporting on its activities and operations, and through other means of public reporting by the Minister (SIRC, 1995, p. vii).

To establish a diverse structure of accountability mechanisms for CSIS, responsibility for accountability was divided across the three branches of government (Weller, 1988, p. 422); executive review would be provided with an independent review body; legislative oversight through Ministerial oversight and Ministerial accountability to parliament and the public; and judicial oversight through the established system of law in Canada, including the Federal Court

of Canada (McDonald, pp. 422, 424-425, 556). The Pitfield Report (1983) further underscored the need for a security intelligence service in Canada that incorporated the different branches of government, including in its three recommendations that there be an increased role for the judiciary when the agency sought to engage intrusive investigative techniques (para. 109), that there be a system in place that is responsible for reviewing the new agency's activities (para. 109), and that the Minister bear the "political responsibility" for the new agency (para. 78).

To ensure effective Ministerial oversight of CSIS, particularly because of when it occurs in the decision-making process, the Minister must have "prior and current knowledge of activities" (Farson, 2000, p. 228). This has been supported by case decisions from the FC, where it was found that the Minister must be informed before he or she can authorize activities conducted by departments or agencies in their portfolio (Canada: R. v. X (Re), 2017 FC 1048). When the CSIS accountability framework was developed, Ministerial oversight was a central component of the processes providing checks and balances to CSIS. Today, Ministerial oversight continues plays a significant role in the accountability framework for CSIS and has acted as a template for how oversight is conducted for other Canadian NSI agencies.

Conclusion

The establishment of CSIS in 1984 and subsequent implementation of the accountability framework altered the landscape for NSI activities conducted in Canada. Figure 1 (see next page) sets out the original framework for CSIS established in 1984, which spanned all three branches of government and held CSIS accountable through several complex mechanisms. Each of these areas across the Canadian governance structure continue to formulate the basis of the accountability framework for CSIS, each playing an integral role in ensuring that the powers and authorities CSIS has been granted are not used in an unnecessary or unreasonable manner.

The remainder of this report will examine how CSIS's oversight and accountability regime has changed over the last thirty-five years. Figure 1 portrays the 1984 accountability framework for CSIS while Figure 2 (see next page) illustrates the analytical framework for the same time period, both of which will be the point of departure for discussing all of the findings.

FIGURE 1: 1984 Accountability Framework for CSIS

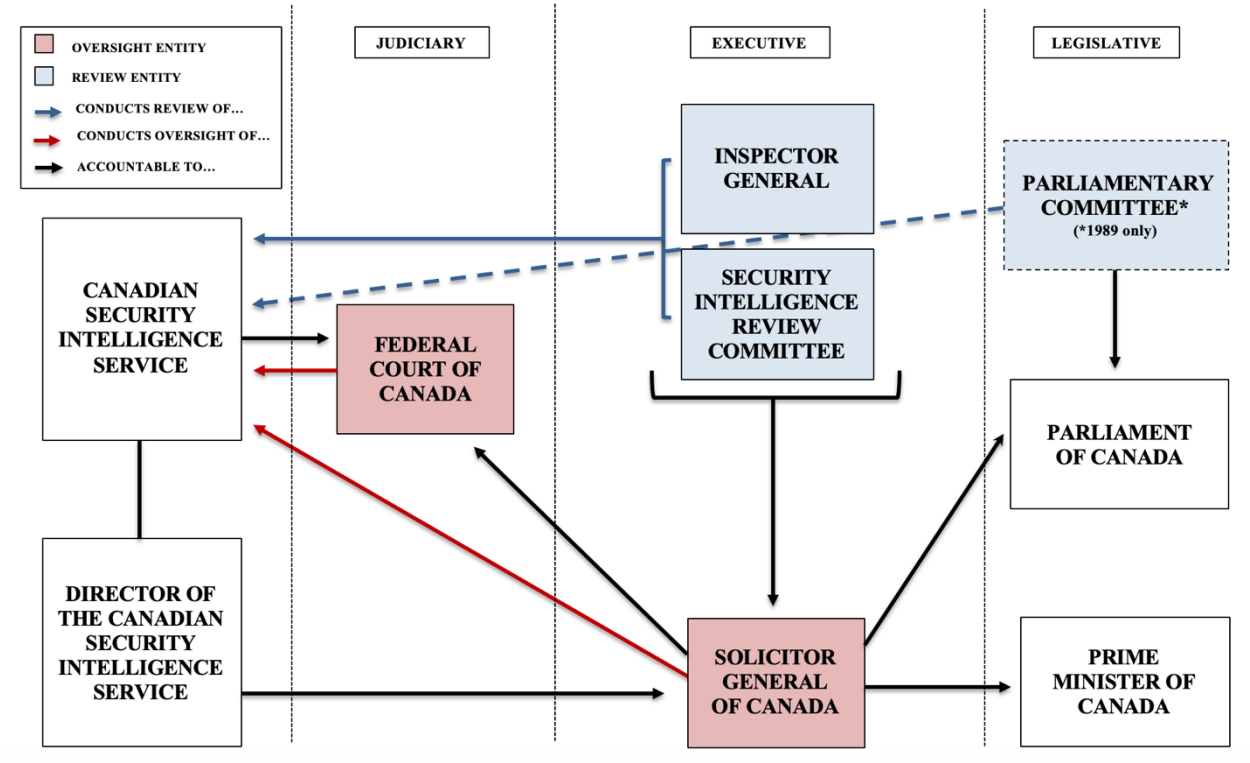
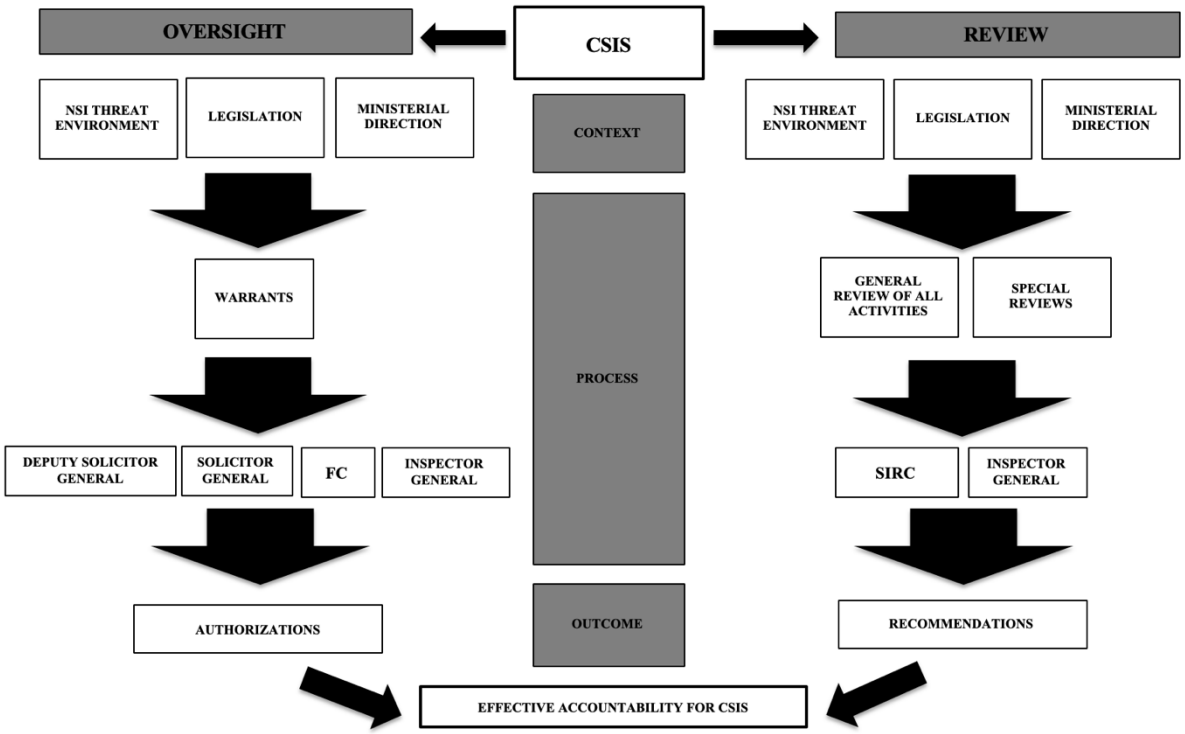


FIGURE 2: 1984 Analytical Framework for CSIS



3. METHODOLOGY AND METHODS

This project provides a comparative historical analysis and analytical framework to Public Safety Canada, with the aim of improving understanding of the role of the responsible Minister, including identifying the parameters regarding Ministerial oversight and accountability. This will be examined alongside past and current environmental contexts and look at how these contexts may have impacted the evolution of the framework.

The primary research question animating this report is:

> *Following the McDonald Commission reports in 1979 and 1981, and the consequent establishment of CSIS in 1984, how has the evolution of the national security accountability framework impacted the role of Ministerial oversight of CSIS?*

Three subsidiary research questions are:

A. To what extent will future changes to legislation of CSIS through the *National Security Act* impact the role of Ministerial oversight for CSIS?

B. Given the changes coming into force, what are possible implications to Ministerial oversight of CSIS and the national security accountability framework?

C. What can be learned from past changes to the national security accountability framework and Ministerial oversight of CSIS, and how these lessons apply to the new framework?

Public Safety Canada will use the information generated in the literature review, as well as the developed framework, to support the Minister in their responsibilities and inform the development of policy for accountability and oversight of CSIS in the future.

Methods

The research methods used in this report include comparative analysis and narrative inquiry. Both the client and the researcher believed these research methods were the best suited for the intent and scope of the research project. Given the unclassified nature of the project, the inclusion of a comparative analysis would provide background and context for answering the above questions, while the narrative inquiry would provide additional depth to these answers through information shared from the participants' direct experiences.

Comparative Analysis

The purpose of the comparative analysis is to understand how the accountability framework for CSIS has evolved since the McDonald Commission and the implications this has had for the role of Ministerial oversight. Comparative analysis was conducted by the compilation of multiple sources, produced both by government organizations and by organizations external to government. All information contained within this report is publicly available and unclassified. Gathering information from multiple sources allowed for a diversity of information and perspectives to be reviewed and analyzed.

Research for this paper included information from the following sources:

1. Academics and research institutions;
2. Government reports from relevant departments and agencies (including Royal Commissions of Inquiry, public reports from CSIS, SIRC and other relevant government agencies in Canada);
3. Legal decisions from the Canadian judiciary system;
4. Reports, documents, materials from international government institutions, such as the USA and the UK;
5. Media reporting to provide historical, contextual information about CSIS, public perception of NSI issues, etc.;
6. Legislation and policy instruments for CSIS, including Acts of Parliament, Ministerial Directions, and Cabinet directives related to oversight and accountability; and,
7. Transcripts of evidence and testimonials given to Parliamentary Committees (both in the Senate and the House of Commons).

Interviews

The purpose of interviewing current and former intelligence and national security staff was to identify key elements of the role of Ministerial oversight and accountability for CSIS, including functions, responsibilities, and organizational structure. The interviews were to be conducted with two groups of individuals:

- Current employees in the Government of Canada who held or currently have a role in one of the entities to the accountability framework for CSIS.
- Former employees in the Government of Canada who worked in one of the entities that contributes or formerly contributed to the accountability framework for CSIS.

Both groups would have knowledge and experience working in the research subject area, but, to be interviewed, needed to have a minimum of three months experience working in this area.

The same questions were asked of all participants. To promote candour and protect the privacy of those interviewed, all participants were granted anonymity.

Limitations of the Methods

This study has three limitations. The first and most important limitation concerned the information gathered in the interviews was the size of the participant groups. Only three individuals, all current employees in the Government of Canada, participated in the interviews. This meant the overall participant group lacked organizational diversity and limited the amount of information that could be gathered.

The second limitation was that of the two participant groups identified as of interest at the outset of this research, only participants currently employed by the Government of Canada were

interviewed. The reason for this lack of take-up was primarily due to the timing of the interviews during the summer months.

The final limitation, while not compromising the findings, was that all information shared in this report is available to the public and unclassified. However, candour was encouraged during the interviews to the fullest extent possible to inform a more comprehensive understanding of the accountability framework and Ministerial oversight.

Conclusion

While this project was partly limited by the number of interviews conducted, the information obtained from the interviews was invaluable to understanding how the framework works from an operational perspective. The unclassified nature of the report meant there was a large quantity of information available publicly to provide a significant foundation for the findings of this report.

As a result of this methodology, the findings within this report will accomplish two things: first, the findings will provide Public Safety Canada with an in-depth foundation of information that can be used for future development of policy in this area; and second, the research will serve to enhance the understanding within the Canadian public about how CSIS is held accountable.

4. FINDINGS: EVOLUTION OF CANADA'S NSI ACCOUNTABILITY FRAMEWORKS

To ensure the success of the CSIS accountability framework when first established, significant consideration was given to what entities should be established in order to maintain the accountability and the credibility of CSIS within the Canadian and international NSI communities. While changes have been made to this framework in the last thirty-five years, the most comprehensive taking place in 2019, the need for this structure for accountability has never been questioned. In fact, the question has primarily been about how much accountability and oversight is necessary for CSIS, while balancing the CSIS mandate to protect the safety and security of Canada.

For many years after its inception, the accountability framework for CSIS was considered one of the best NSI accountability-framework models in the world. In 1999, a former Solicitor General of Canada testified to both the whole-of-government approach and the framework's transparency during a Senate Committee hearing, stating that the accountability framework for CSIS was a model other countries wished to implement (Farson, 2000, p. 225). This is because the framework has accountability mechanisms in each of the executive, legislative and judicial branches of government, ensuring a multi-faceted, whole-of-government approach to holding CSIS accountable. It also stood out because the accountability framework was made accessible to the public through legislation.

In 1984, CSIS's accountability framework consisted of the following entities: the responsible Cabinet Minister, SIRC, the Inspector General, and the FC. The framework was supplemented by a one-time legislated review conducted by a special parliamentary committee in 1989, five years after CSIS was established (CSIS Act, section 56). This review led to small, non-legislative changes to the roles of the Minister and to the Director of CSIS (the deputy head of the new agency), including increased public reporting to increase the degree of accountability for the agency. However, the majority of recommendations arising from the parliamentary review were not adopted by the Government. Following this Parliamentary review, legislation and the overall accountability framework for CSIS went unchanged for nearly thirty years until the first, most significant alteration to the accountability framework occurred in 2012.

Between 1984 and 2012, CSIS was gradually granted a significant increase in powers and authorities to carry out its statutory mandate to deal with an evolving threat environment, the most notable was the passage of the *Anti-terrorism Act* in 2001. This increase in authorities granted to CSIS preceded an expansion of the policy portfolio for the responsible Minister; first, consolidating several departments to create the Department of Public Safety and Emergency Preparedness (Public Safety Canada) in 2003 and later the creation of the Canada Border Services Agency (CBSA) in 2005. The positive and negative implications of the expansion of the Minister's portfolio continue to reverberate into the present context of 2019.

The dissolution of the Inspector General in 2012 marked the first major change to the accountability framework for CSIS after nearly 30 years of operating in the same review and oversight context. This further impacted the extent of responsibilities of the Minister in the CSIS accountability framework, since the responsibilities of the Inspector General were reallocated to

the Minister and to SIRC. The result was that these entities held more responsibilities without necessarily being granted additional supports to aide them.

A series of legislative changes in the years following the elimination of the Inspector General role generated further change to the CSIS accountability framework. Legislation passed in 2017 and 2019 altered the accountability framework, providing a mechanism for parliamentary review with the new NSICOP in 2017, and then a complete reformation of the accountability framework in 2019 with the passage of the *National Security Act, 2017*. Despite these legislative changes to the accountability framework, the role of Ministerial oversight – the most direct oversight mechanism in the framework – remained as a pivotal component for holding CSIS accountable.

The process for developing the *National Security Act, 2017* began with a round of large-scale stakeholder engagement sessions in late 2016, based on the discussion paper *Our Security, Our Rights: National Security Green Paper, 2016*. Their purpose was to gather input from a variety of Canadian stakeholders, including the public, experts, and public institutions, which would help policy makers develop legislation that serves as "an appropriate balance" (Government of Canada, 2016, p. 6) between actions taken to protect Canadians and actions that could infringe on the rights laid out in the *Canadian Charter of Rights and Freedoms*. One of the measures used to assess this balance was through the established accountability framework. The paper looked at several areas related to national security, but stakeholders identified accountability for national security agencies as a major concern.

The *National Security Act, 2017* focused mainly on two key areas: enhancing transparency and accountability within the national security apparatus, including clarifying the role of and the activities conducted by CSIS; and amending legislation to better reflect the current threat environment while ensuring the national security community remains capable of evolving to meet a changing threat environment (ITAC, 2018, p. 25). For CSIS specifically, the *National Security Act, 2017,* amended aspects of the CSIS Act, including providing clarification of the CSIS threat reduction mandate as well as create new methods for ensuring accountability (ITAC, 2018, p. 25). Part of the proposed changes to the accountability framework included creating of the National Security and Intelligence Review Agency (NSIRA) and the Intelligence Commissioner, both of which will serve to address "long-standing problems related to review [of CSIS]" (SECU Evidence, December 5, 2017).

Following the passage of the *National Security Act, 2017,* the accountability framework for CSIS consists of the following entities: the responsible Cabinet Minister, NSIRA, the NSICOP, the Intelligence Commissioner, and the FC. This formal framework is also supported by a parliamentary committee in each of the House of Commons and the Senate.

This section will first look at the different components incorporated in the accountability framework over the last thirty-five years, examining each in turn. The goal is to provide context to better understand the evolution of the accountability framework. This is supported by Table 2 (see next page), which illustrates at a high-level the role of each of the main entities within the framework.

TABLE 1
Comparison of Accountability Functions for Canadian NSI Agencies (1984-2019)

Agency	Review	Oversight
Inspector General	X	X
Intelligence Commissioner	X	X
National Security and Intelligence Committee of Parliamentarians (NSICOP)	X	
Security and Intelligence Review Committee (SIRC)	X	
National Security and Intelligence Review Agency (NSIRA)	X	
Cabinet Minister (Minister of Public Safety and Emergency Preparedness)		X
Federal Court of Canada (FC)		X

(Retrieved and adapted from Leuprecht & McNorton, 2018)

Accountability Framework: Oversight

Cabinet Minister (Solicitor General, 1984-2003; Minister of Public Safety and Emergency Preparedness, 2003-Current)

Ministerial oversight is an integral function of the accountability framework for CSIS, as demonstrated by the minimal changes made to the role and function since CSIS was created in 1984. Ministerial oversight is the primary mechanism to ensure legislative and parliamentary accountability for CSIS, though the Minister also has certain review functions that remain a central part of the Minister meeting their accountability responsibilities. While some responsibilities have been delegated to the deputy heads of CSIS and Public Safety Canada, the Minister is ultimately accountable for the activities conducted by CSIS.

Ministers are held accountable through their responsibility and answerability to Parliament, parliamentary committees, and the Prime Minister of Canada, as the Cabinet Minister who appoints them to Cabinet (Smith, 2006, pp. 112, 115). Ministers, when appointed members of the Cabinet, assume authority of their portfolios upon taking an oath of office and simultaneously

become accountable for the portfolio as well (Smith, 2006, p. 118). When CSIS was established in 1984, it was placed into the ministerial portfolio of the Solicitor General of Canada. Nearly two decades later, in 2003, significant departmental reorganization led to the dissolution of the Department of the Solicitor General and the creation of the new Department of Public Safety and Emergency Preparedness, simultaneously re-named the Solicitor General to the Minister of Public Safety and Emergency Preparedness (the Minister) (Office of the Auditor General of Canada, 2004, para. 3.12).

Despite these organizational changes, the role Ministerial accountability plays for CSIS has remained the crucial foundation for holding CSIS accountable. The Minister holds multiple authorities to ensure that CSIS complies with the law, the most important being oversight of CSIS activities and the responsibility that accompanies it. To effectively wield this authority, the Minister must be apprised of all practices, policies, and operations CSIS undertakes, particularly when these activities might have issues related to policy or the law (McDonald, 1981, p. 408). The scope of the Minister's authorities is an important component of the Minister's ability to be accountable to Parliament and the Canadian public, particularly since they have the potential to impact the lives of individuals in Canada. One such authority is that the Minister can issue regulations and directives to CSIS, as per subsection 6(2) of the CSIS Act.

One known use of this authority specific to oversight of CSIS operations is the 2015 Ministerial Direction for Operations and Accountability. This Ministerial Direction replaced two preceding Ministerial Directions issued in 2008 and 2001 on the same subject (Government of Canada, 2015, p. 2). The redacted version of the Ministerial Direction, made available to the public by the recipient of an Access to Information request, outlines the responsibility of the Director of CSIS to keep the Minister informed of any issues or when the directions issued under the Ministerial Direction have been disregarded (Government of Canada, 2015, p. 3). The Ministerial Direction also details the primary principles for how CSIS activities are to be conducted and how CSIS will be kept accountable for these operations (Government of Canada, 2015, pp. 2-3). An unredacted version of this Ministerial Direction has not been made available to the public.

The requirement for Ministerial authorization was built into the founding legislation of CSIS, derived from the recommendations of both the McDonald Commission and the Pitfield Report. The rationale for this stipulated that CSIS activities must be conducted in compliance with the law and, if met certain thresholds, that the activity is strictly necessary to fulfill CSIS's mandate. This is the foundational premise of Ministerial accountability, complicated by the complexities associated with NSI agencies and their activities.

An example of an activity requiring Ministerial authorization is the application to the FC for a section 21 warrant under the CSIS Act. The responsible Minister must be held accountable for "each intrusion upon the reasonable expectation of privacy of a person" (Canada: R. v. X (Re), 2017, FC 1048), which includes activities conducted under warrant. To authorize warrant applications, the Minister must be made aware of all relevant information in order to "understand the factual nexus between the relevant threat to the security of Canada and the person(s) whose privacy interests will be intruded upon" (Canada: R. v. X (Re), 2017, FC 1048). However, the idea that the Minister must be fully aware in order to authorize certain activities and then be held accountable for it, contrasts with the findings of the McDonald Commission, which stated there

was an expectation that Ministers might not know everything about all current activities or operations of CSIS (McDonald, 1981, p. 672).

It is possible for the Minister to meet this threshold for understanding through various legislated means. First, the Minister receives direct reports from the Director of CSIS, who is statutorily mandated to provide the Minister with a report on CSIS operational activities whenever the Minister requests a report (CSIS Act, subsection 6(4)). Second, the Minister is provided information from SIRC (now NSIRA) through both their annual reports and briefings, the latter of which is required to occur at minimum once per year, or more frequently if the Minister requests. Third, the Deputy Minister of Public Safety, who must be consulted by the Director of CSIS on certain activities outlined in legislation, can provide the Minister with advice or recommendations regarding Ministerial directions issued by the Minister to CSIS.

While most of the Minister's accountability responsibilities for CSIS are captured in legislation, the role of Ministerial oversight of CSIS is still considered broad and complex. Due to the complexities associated with NSI agencies, there is a balance the Minister must meet when engaging CSIS and vice versa (Wark, 2015, p. 6). For Ministers to be effective decision-makers when matters for consideration are presented to them by CSIS requires that the Minister to understand the context in which CSIS operates; yet, there may also be a desire for the Minister to remain distant and engage in a practice of "plausible deniability" (Wark, 2015, p. 6). One way this can be achieved is that deputy heads, including the Deputy Minister of Public Safety Canada, are delegated certain decision-making authorities by the Minister, which prevents the Minister from being regularly advised about some activities and operations (SIRC, 2014, p. 19).

With the passing of the *National Security Act, 2017* in June 2019, the scope of oversight and review responsibilities for the responsible Minister for CSIS have been further clarified and in some cases increased (SECU Evidence, December 5, 2017). After the Inspector General was eliminated, there was a lack of legislative clarity for the Minister regarding the transference of the review and certification functions once the responsibility of the Inspector General. Establishing NSIRA and the Intelligence Commissioner with their statutory Acts provides the Minister with specific obligations and procedures related to oversight of CSIS operations and activities.

TABLE 2
Ministerial Authorities & Oversight Mechanisms in the *CSIS Act* (prior to the *National Security Act, 2017)*

POWERS AND AUTHORITIES
• Section 6(1): Director of CSIS serves under the direction of the Minister • Section 6(2): Authorizes issuance of Ministerial Directions to the Director of CSIS • Section 13(2) and (3): Minister must approve arrangements with Canadian provinces and territories, and foreign states, regarding the provision of security assessments to the arranged entity

Deputy Minister of Public Safety Canada (1984-Current)

With respect to CSIS, the primary function of the Deputy Minister for matters related to accountability is to support the Minister by keeping them informed in order to effectively carry out their responsibilities related to CSIS. The CSIS Act mandates that the Director of CSIS consult with the Deputy Minister on general operational policies of CSIS, on matters related to warrant applications under sections 21, 21.1 and 23 under the CSIS Act, and other matters that the Minister has directed them to consult on, per Ministerial directions (CSIS Act, subs. 7(1-3)). The goal is to ensure that the advice provided to the Minister on these activities provides each with the necessary understanding needed to perform their respective oversight functions under the accountability framework (Narrative inquiry, 2019).

Inspector General (1984-2012)

Although the Inspector General was not a role recommended by the McDonald Commission, it, was added as the CSIS Act was developed and then considered an innovative role, given the joint review and oversight functions. When the Inspector General was first established, it did not have a similar counterpart in other countries. Since, the Inspector General in Canada counterparts did emerge among Canada's allies; several nations like the UK, the USA, and Australia introduced accountability frameworks with several Inspector General-like entities.

For nearly thirty years the Inspector General supported Ministers in the carrying out their oversight role by performing supplementary review, assessing CSIS compliance with the law and issuing certificates of satisfaction with their compliance. The Inspector General could conduct the latter due to its legislated monitoring function, looking specifically at matters of operational compliance (Cronk, 1985, p. 7). If the Inspector General was satisfied that there were not any instances in which any activity conducted by the agency was "unauthorized, unreasonable or unnecessary" (Pitfield, 1983, para. 89), the Inspector General would provide the Minister with a certificate indicating this satisfaction. If any circumstances were identified that met the above criteria, the Inspector General was required to note this in their annual certification to the Minister (SIRC, 1988, p. 69). However, unlike the annual SIRC reports, certificates issued by the Inspector General were not disclosed publicly (Whitaker, 1992, p. 58).

The other function of the Inspector General was conducting reviews of CSIS. While SIRC was designed with a strictly external review mandate, the intention for the Inspector General was to conduct internal reviews of CSIS, as well as review the annual reports from both CSIS and SIRC. They were also able to coordinate reviews or conduct investigations as directed by SIRC, should the instance arise (SIRC, 1985, p. 4).

In 2012, the Inspector General role was discontinued. Its roles and responsibilities were reallocated to different areas of the CSIS accountability framework (Senate Committee on National Finance, 2012; Government of Canada, 2013, p. 57). The dissolution about as part of the Deficit Reduction Action Plan from the 2012 Federal Budget, which sought to increase the efficiency and streamline processes for CSIS (Government of Canada, 2013, p. 57).

Intelligence Commissioner (2019-Current)

The Intelligence Commissioner was created in 2019, an additional entity to oversee certain CSIS activities. Unlike the former Inspector General, the Intelligence Commissioner is mandated to determine the reasonableness of Ministerial authorizations for certain CSIS activities (such as the collection and retention of datasets) and in some cases authorizing these activities, as well as examining related Ministerial directions and legislated authorities (SECU Evidence, April 23, 2018). The Intelligence Commissioner is also responsible for overseeing the Communications Security Establishment (CSE). The Intelligence Commissioner must be a retired judge from a superior court (Intelligence Commissioner Act, subsection 4(1)). At the time of writing, the Intelligence Commissioner does not have a counterpart amongst Canada's Five Eyes allies (SECU Evidence, December 5, 2017).

Federal Court of Canada (1984-Current)

The final facet of oversight for CSIS involves the judiciary and is handled by the FC. Since 1984, the FC contributes to oversight of CSIS in two primary ways: first, by reviewing and authorizing warrant applications submitted by CSIS; and second, by identifying issues with certain CSIS activities and possible gaps in relevant legislation.

The FC is responsible for assessing and authorizing warrant applications from CSIS. The warrants are for the authorization of what Pitfield (1983) referred to as extraordinary powers and capabilities, both considered necessary for the new security intelligence service to successfully fulfill their legislated mandate and to avoid any possible abuses of power by the agency (paras. 56-57). In a 2017 FC decision, the FC described the role of judicial oversight as being a position designed not "to decide on the importance on a national security matter… [but to decide] whether other methods are available, whether the belief is reasonable or probable… [and] whether additional terms and conditions should be imposed" (FC Decision, 2017, section 44). In other words, the FC ensures any activity carried out by CSIS that requires a warrant is lawfully authorized and it is the Minister, as the holder of the relevant knowledge of the national security context, who is responsible for making a decision regarding national security priorities.

When CSIS requests a warrant authorization and the Minister approves it, the judiciary is responsible for ensuring that the warrants are issued only if legal requirements have been met and that there are no *Charter* infringements (Green Paper, 2016, p. 10). Warrant applications can be refused if the FC is not satisfied that there is sufficient justification. While the Minister is accountable for the activities authorized in the warrant request, the judge or judges presiding over the warrant application requests still need to be satisfied that there is a justification for authorizing the intrusion into an individual's privacy, such as a demonstration of the gravity of the security threat, and that the circumstances are "specific and exigent" (Pitfield, 1983, para. 60; Canada: R. v. X (Re), 2017 FC 1048).

The FC has also contributed to accountability of CSIS by identifying issues related to CSIS carrying out certain activities under their legislated mandate. For example, in 2016 *Canada v. X(Re)* the FC found that CSIS was not in compliance with the law and had conducted activities for several years that went beyond the limits established by the CSIS Act in 1984 (2016 FC

1105, p. 123). The *National Security Act, 2017*, which amended certain sections of the CSIS Act, seeks to resolve this issue identified by the FC (Narrative inquiry, 2019).

Accountability Framework: Review

Security Intelligence Review Committee (1984-2019)

SIRC was the first external review body to undertake general and special reviews of CSIS activities and performance, including measures taken to reduce threats to the security of Canada (*Canadian Security Intelligence Service Act* [CSIS Act], 1985, section 38). Established in 1984 with the CSIS Act, SIRC was considered the "only truly independent external review" (Rempel, 2004, p. 637) entity in CSIS's accountability framework and complemented the internal reviews of the Inspector General (Rankin, 1986, pp. 257-258).

SIRC was mandated to perform three roles: first, to function as external executive review for CSIS; second, to examine any complaints made about CSIS activities; and third, resolve issues related to security clearances for federal employees and those in the public seeking to provide services or goods to the federal government (SIRC, 1985, p. 2). Members of SIRC were appointed by the Governor in Council and could not be active members of the Senate or House of Commons (SIRC, 1985, p. 1); however, SIRC members were traditionally appointed to reflect the proportion of each major party in the House of Commons when appointments were made (Chalk & Rosenau, 2004, p. 30). This, combined with its responsibility to submit a report annually to the House of Commons, earned the committee the nickname of "Parliament's watchdog" (SIRC, 1986, p. 3).

SIRC's original mandate included annual reporting on the activities of CSIS, considering "laws, regulations and rules of evidence, as well as the applicable case law in similar cases" (Canada (Attorney General) v. Al Telbani, 2012, para. 62, p. 17). SIRC could, if appropriate, provide recommendations on the basis of their reviews; however, CSIS does not have to accept SIRC recommendations since the recommendations "do not have the force of a decision" (Canada (Attorney General) v. Al Telbani, 2012, para. 62, pp. 17-18), and consequently do not have to be considered directives. To conduct their reviews, SIRC was granted access to information controlled by CSIS on how it performed its duties and functions (CSIS Act, 1985, section 39(2)).

The elimination of the Inspector General in 2012 led to several changes in the responsibilities for SIRC. First, the certification of satisfaction would be completed by SIRC and these certificates would be sent directly from SIRC to the responsible Minister. Second, the CSIS Annual Report had to be submitted to SIRC as well as the Minister. Third, SIRC would brief the responsible Minister at least once annually on CSIS matters (Senate Committee on National Finance, 2012). SIRC publicly expressed some initial concerns about maintaining the ability to conduct independent review with these new responsibilities in its 2011-2012 annual report. However, SIRC reported in 2014 that these concerns were unfounded, and that the role of SIRC in the accountability framework benefited from these new responsibilities (SIRC, 2014, p. 10). Under the *National Security Act, 2017*, SIRC was formally dissolved in 2019 and a new NSI review agency, NSIRA, was established.

National Security and Intelligence Review Agency (2019-Current)

NSIRA was established under the *National Security Act, 2017,* which represents the largest systemic reorganization of the accountability framework for NSI since CSIS and its oversight and review bodies were established in 1984. The *National Security Act, 2017* consisted of nine parts, each addressing entities in the NSI community, and included amendments to the CSIS Act to clarify the scope of activities the NSI agency can conduct on behalf of Canada's national security and the protection of Canadians from threats. However, a significant portion of the *National Security Act, 2017* focuses on ensuring that these activities have appropriate review and oversight mechanisms, and that agencies, including CSIS, are held accountable.

The largest new accountability mechanism under the new act is NSIRA, which absorbed the responsibilities of SIRC and Office of Communications Security Establishment Commissioner (OCSEC) and serves as the primary review entity for both. NSIRA must also review or investigate NSI matters within other departments or agencies across government (NSIRA Act, s. 8(1)). Like SIRC, any findings or recommendations from NSIRA, including those related to compliance with the law and applicable Ministerial directions, and the "reasonableness and necessity of a department's exercise of its powers" (s. 8(3a-b)), can be provided as NSIRA determines. As well, NSIRA will not have access to information containing Cabinet confidences but will have access to all other kinds of information for conducting comprehensive reviews of the NSI community and their activities (SECU Evidence, April 17, 2018). Table 2 (see next page) provides a comparison of both SIRC and NSIRA.

National Security and Intelligence Committee of Parliamentarians (2017-Current)

The creation of the NSICOP in late 2017 was the first in a series of significant reforms to the CSIS accountability framework. While the name and membership of current members of parliament suggests that the NSICOP is a committee of Parliament, the NSICOP remains fully separate from Parliament and is subject to fulfilling the mandate in the *National Security and Intelligence Committee of Parliamentarians Act* (the *NSICOP Act*).

The NSICOP is to provide a non-partisan, non-parliamentary entity to conduct review of the activities conducted by NSI agencies, including CSIS, as well as review "legislative, regulatory, policy, administrative and financial framework[s]" (*National Security and Intelligence Committee of Parliamentarians Act* [NSICOP Act], 2017, ss. 8(1)(a)) for the NSI community and review matters any Cabinet Minister may refer to the Committee (NSICOP Act, 2017, ss. 8(1)). While SIRC requires its members not to be sitting members of either House of Parliament, the NSICOP consists only of members sitting in either the House of Commons or the Senate, though they cannot be a Cabinet Minister or parliamentary secretary (NSICOP Act, ss. 4(1-3)).

TABLE 3
Organizational Comparison between SIRC and NSIRA

	Security Intelligence Review Committee	**National Security and Intelligence Review Agency**
Mandate	● Review ● Investigate complaints	● Review ● Investigate complaints
Responsible for Review of these Departments/ Agencies	● CSIS	● CSIS ● CSE ● Any department or agency that carries out activities related to national security or intelligence
Members	● 2-6 members ● Governor in Council appoints members from those who are members of the Queen's Privy Council ● Members cannot be members of House of Commons or Senate ● Appointed after consultation by the PM with Leader of the Opposition and the leader of parties in the House of Commons with at least 12 members ● Members limited to serving a maximum of two terms (each term is 5 years)	● 3-7 members ● Governor in Council appoints members ● Appointed after consultation by the PM with Leader of the Opposition and the leader of parties in the House of Commons with at least 12 members ● Members are limited to serving a maximum of two terms (each term is 5 years)
Reporting	● Annual report to appropriate Minister (to be submitted no later than September 30 of each fiscal year) ● Annual report to Parliament ● Special report to appropriate Minister	● Annual report to appropriate Minister of CSIS ● Copy of report to the Intelligence Commissioner (if report relates to IC powers, duties or functions) ● Annual report to PM (public) ● Compliance reporting to the Attorney General of Canada ● Annual report to Minister of Public Safety and Emergency Preparedness for SCIDA (public) ● Special report to appropriate Minister on any matter that is in the public interest (public)
Access to Information	● All but confidence of the Queen's Privy Council	● All but confidences of the Queen's Privy Council

Powers	● Review performance of CSIS ● Review measures taken by CSIS to reduce threats to the security of Canada ● Review Ministerial directions issued to CSIS ● Review information and intelligence sharing arrangements CSIS enters into ● Provide certificate to Minister about satisfaction with both CSIS conduct and CSIS report ● Compile and analyze operational activity statistics (i.e. number of warrant applications) ● Investigate complaints (security clearances) made against CSIS	● Review any activity or matter related to national security or intelligence ● Review measures taken by CSIS to reduce threats to the security of Canada ● Review Ministerial directions issued to CSIS, CSE or a department/agency, if the direction is related to NSI ● Investigate complaints (security clearances) made against CSIS or RCMP ● Provide findings and recommendations to the appropriate entity
Coordination	● Inspector General (prior to 2012) ● Auditor General of Canada ● Privacy Commissioner of Canada	● Civilian Review and Complaints Commission for the RCMP (CRCC) ● Attorney General of Canada (compliance reporting) ● Privacy Commissioner of Canada ● Auditor General of Canada ● Any other relevant review entity responsible for reviewing a department or agency

(Adapted from the *CSIS Act*, 1985 and the *NSIRA Act*, 2019)

While the NSICOP does not conduct direct parliamentary oversight or review, as previously suggested by the McDonald Commission and other experts in this field, NSICOP introduced a form of parliamentary review of CSIS activities for the first time since the one-time legislated review of the *CSIS Act* in 1989 by a parliamentary committee. However, there are some logistical limitations, including the NSICOP being subject to strict parameters around information they can access (e.g. records containing Cabinet confidences or information about ongoing investigations) (NSICOP Act, 2017, s. 14).

Standing Committees of Parliament: Senate and the House of Commons

The role of Parliament and Parliamentarians in the CSIS accountability framework has been contentious since the 1980s. Unlike other allied nations, including the UK, the USA, and Australia, Canada has maintained minimal parliamentary involvement in the accountability framework for CSIS. While there was a legislated mandate for a parliamentary committee to conduct a review five years after CSIS was established, there was no formal mechanism for Members of Parliament to conduct review of the agency until the establishment of the NSICOP in 2017, though even the NSICOP has limited parliamentary function.

Prior to the NSICOP, Parliament elected to establish a "permanent subcommittee on national security" (Whitaker, 1996, p. 282) in 1990 following the first mandated review of the CSIS Act. However, this committee elected not have the requisite security clearance that SIRC had, thus limiting their access to information and forcing them to rely on SIRC to conduct a more comprehensive review of CSIS (Whitaker, 1996, p. 282). In 2019, two standing committees in the Senate and the House of Commons are mandated to address NSI matters, including specific policies, legislation, and programs, within their respective responsibilities: the House of Commons Standing Committee on Public Safety and National Security (hereafter SECU), and the Standing Senate Committee on National Security and Defence (hereafter SECD) (House of Commons Standing Committee on Public Safety and National Security [SECU], n.d.). Since neither committee formally conducts "regular monitoring of activities and operations" (Rempel, 2004, p. 647), nor do committee members have the requisite security clearances needed to review certain information, it difficult is for them to conduct effective or comprehensive reviews.

SECU, established as a standing committee of the House of Commons in 2001, is mandated to conduct reviews of federal departments and agencies that are responsible for national security policy, programs, and financial expenditure plans (SECU, n.d.). In 2006, SECD was established as a standing Senate committee to conduct studies of issues related to national security, intelligence and defence, as well as conduct examinations of legislation related to these issues (Standing Senate Committee on National Security and Defence [SECD], n.d.).

Special Committee on the Review of the CSIS Act and the Security Offences Act (1989)

This mechanism for parliamentary review of CSIS was built directly into legislation, providing a statutory mandate for a parliamentary committee to conduct a review of the CSIS Act five years after it was established. This five-year review was the only parliamentary review or oversight of CSIS prior to 2017, despite the McDonald Commission's recommendation. As Pitfield notes in the Special Senate Committee report (1983), there were concerns about the influence of

partisanship and political interference by such a parliamentary committee, as well as a duplication in review authorities between SIRC and this committee (para. 100). However, it was agreed that a one-time review by a parliamentary committee should occur after five years of CSIS's existence.

The Special Committee on the Review of the *CSIS Act* and the *Security Offences Act* was formed in early summer 1989 and released its findings a year later (Rosen, 2000). The report, *In Flux but not in Crisis*, detailed 117 recommendations for the two Acts. In particular, there were recommendations on further defining the roles of SIRC and the Inspector General and establishing a sub-committee of parliament that could monitor and review the broader Canadian security and intelligence community (Rosen, 2000; Farson, 1996). Despite the Special Committee's many recommendations, Farson (1996) noted that they were made without the Special Committee having access to certain information, including the annual reports from SIRC, CSIS and the Inspector General, and any Ministerial directions issued since CSIS was first established. This made it challenging for the Special Committee to make recommendations based on a comprehensive review of certain operational procedures and directives (Farson, 1996).

None of the recommendations of the Special Committee were adopted by the Government, stating that no legislative changes were required; however, the Government did agree to adapt existing roles and reporting requirements to provide Canadians with more information about national security threats and thus increase the public's capacity to hold CSIS accountable (Rosen, 2000). Beginning in 1992, the Government established a public reporting mechanism for the Director of CSIS, provided the public with an annual Ministerial statement on NSI issues and threats, and released a breakdown of the budget for CSIS (Rosen, 2000). Each of the above mechanisms have remained in place since their adoption in 1992 and continue to play a role in the accountability framework to this day.

As described above, attempts made by previous parliamentary committees were unsuccessful in incorporating any further parliamentary review or oversight mechanisms. However, there continue to be advocates for the incorporation of regular parliamentary review of departments and agencies across government, including Guerin, McCrae and Shepheard (2018), who state that accountability for government institutions (though not specifically NSI agencies) can only be improved by increased parliamentary scrutiny (p. 4).

Conclusion

Canada's accountability framework for CSIS was designed to ensure accountability for the new NSI agency was accomplished across government, developing a multi-faceted system to conduct oversight where certain rights or freedoms would be impacted, and to regularly review these extraordinary activities to act as a supplement to the established oversight bodies. The recent changes to the accountability framework for CSIS mark the most extensive structural changes since 1984, and will have impacts across the entire NSI community, not just CSIS.

Among all of the changes to the CSIS accountability framework since 2012, the role of the responsible Cabinet Minister and the judiciary in conducting oversight of CSIS has remained an integral component of the framework. This appears to be a clear recognition of the importance of

Ministerial oversight and the role of the judiciary in keeping CSIS accountable. For the Minister, their ability to conduct oversight is reliant on their ability to remain as informed as possible in order to be held accountable as a decision-maker and the sole political figure accountable for CSIS. The judiciary, as the final authorizer of certain intrusive activities, holds CSIS accountable for activities that would otherwise contravene the rights and freedoms of Canadians and ensuring that the authorized activities comply with the law.

The overall constancy of CSIS's accountability framework has contributed to the overall stability of the organization and accountability processes, while inadvertently creating challenges for the review and oversight entities under the framework to effectively conduct mandated activities and ensure CSIS is held fully accountable. For nearly 28 years, CSIS operated within the same accountability framework context without experiencing any major changes to the entities charged with ensuring its accountability and compliance with the law. The available literature from SIRC and narrative inquiries describe this stability as beneficial for the agency and the review entities, as it allowed for establishing the processes necessary to keep CSIS accountable and to allow for developing the working relationships between CSIS and the review entities. However, the threat context in which CSIS operates has changed significantly since CSIS was first established and this has different implications for CSIS, from the kinds of activities they conduct to ensure the protection of Canadians to how review and oversight of CSIS is conducted.

5. FINDINGS: International NSI Accountability Frameworks

Canada has long had global intelligence-sharing relationships, the most public of which is the Fives Eyes alliance. The basis for this alliance is the UKUSA Agreement, signed first in 1946 by the United States and the UK, later expanded to include Canada, Australia and New Zealand in 1955 (Kim & Perlin, 2019). However, public acknowledgment of NSI partnerships has varied and, until recently, often gone unacknowledged. The Five Eyes alliance was publicly avowed in 2010, with records of the original UKUSA Agreement and the amended version from 1955 being released by the implicated nations in June 2010 (Kim & Perlin, 2019; National Archives, n.d.).

This section provides a high-level overview on how two of Canada's allies – the USA and UK – in national security and intelligence address accountability for their respective NSI agencies oversight and whether there are any new or innovative elements that Canada could consider. However, with each country having different governance models (e.g. the UK's parliamentary system, which Canada's own system is based upon, still contains different elements and traditions), it would be challenging for Canada to implement each model exactly in a Canadian context without making any changes.

Accountability Framework: United States of America

The Central Intelligence Agency (CIA) was established in 1947 in the USA with an intelligence coordination function, with the statutory mandate to "correlate, evaluate, and disseminate intelligence" from all intelligence agencies in the USA, and ensure the President of the USA was provided this intelligence (Rockefeller, 1975, p. 10). The role of coordinating intelligence for the President was shifted to the new Director of National Intelligence in 2005 following an inquiry into the 2001 terrorism attacks. Since then the CIA's role in the NSI community has focused on the collection and analysis of foreign intelligence (Office of the Director of National Intelligence [ODNI], 2017, p. 1; Central Intelligence Agency [CIA], 2018).

Legislative changes to the accountability framework for the CIA came about as a result of scandals (e.g. Watergate) and the subsequent inquiries into how the agency was held accountable for their activities, including the Commission on CIA Activities within the United States (known as the Rockefeller Commission). The Watergate hearings and the Rockefeller Commission uncovered activities conducted against US citizens, and the subsequent public reaction to the Watergate allegations revealed a lack of public understanding on what activities the CIA could conduct to protect the security and safety of the nation (Rockefeller, 1975, p. 9). What followed was addressing how the USA could balance a system of oversight comprehensive enough to ensure NSI agencies be held accountable with the fundamental purpose of having NSI agencies: protecting the security and safety of citizens (Rockefeller, 1975, p. 14).

Today, accountability for the CIA is handled by two branches of the US government. The legislative branch conducts review and oversight functions primarily through the establishment of special committees in Congress. The executive branch fulfills its responsibilities by establishing Inspectors General for individual agencies, the National Security Council, the President's Intelligence Advisory Board, and the Intelligence Oversight Board (Executive Office

of the President of the United States [White House], n.d.). Oversight and review of the CIA has varied since the agency's creation, but many of the elements remain important.

House of Representatives (Congress)

Congress has long had legislative controls to ensure accountability for the activities conducted by the CIA; however, these controls has not always been consistent or comprehensive enough for holding the CIA accountable. From 1947, Congress served as the primary, though informal, means of oversight for the CIA. The 1975 Rockefeller Commission noted that Congressional subcommittees were only able to review the CIA's budget, and not any of the activities of CIA officials carrying out duties (Rockefeller, 1975, p. 14). The role of Congress was not formalized into legislation until 1980 with the passing of the *Intelligence Oversight Act*. This Act gave the House Permanent Select Committee on Intelligence a mandate to authorize and oversee the programs and activities of the CIA, and an identical mandate to the Senate Select Committee on Intelligence (CIA, 2018).

Inspector General for the Central Intelligence Agency

Since 1989, independent oversight of the CIA has been conducted by the Inspector General for the CIA (Central Intelligence Agency [CIA], 2016). The *Inspectors General Act* of 1978 first authorized creating an Inspector General for the CIA, as well as for other departments and agencies across the US Government. At time of writing, there were 74 Inspectors General across the US Government (Atkinson, 2019, p. 9). The Inspector General of the CIA performs oversight through "independent audits, inspections, investigations, and reviews of CIA programs and operations", and submits all findings and recommendations to the Director of the CIA, the CIA itself, and the relevant committees in Congress (CIA, 2016).

President's Intelligence Advisory Board

Established in 1956, the President's Intelligence Advisory Board has provided oversight of intelligence activities. It offers independent advice regarding two matters: first, the effectiveness and efficacy of intelligence agencies in performing their mandated responsibilities; and second, how intelligence agencies are planning ahead (White House, n.d.). To perform its functions and effectively inform the President, the President's Intelligence Advisory Board has access to all information it requires to perform this function.

Intelligence Oversight Board

The Intelligence Oversight Board was established in 1976 as a result of recommendations from the Rockefeller Commission (White House, n.d.). The Commission was a direct result of the Watergate scandal, which alleged the CIA participated in misconduct and conducted non-legislated espionage activities against US citizens (Rockefeller, 1975, p. 9). The Intelligence Oversight Board undertakes complementary oversight of NSI agencies' compliance with the law and executive directives from the President and informs the President when an activity has taken place that contravenes the law or should otherwise be brought immediately to the attention of the President (White House, n.d.).

Accountability Framework: The United Kingdom

Of Canada's primary NSI allies, the UK is most similar to Canada, in both its Westminster governance system and NSI agency structure. While not identical, many useful comparisons can be drawn for Canada from the way UK governments have held their NSI agencies accountable.

The UK agency that most closely resembles the activities and responsibilities of CSIS is the Security Service (MI5), the domestic intelligence service. This section primarily focuses on MI5, which is held accountable by the legislative, executive and judicial branches of government. The MI5 accountability framework consists of the following: the Secretary of State for the Home Department, the Intelligence and Security Committee, the Judicial Commissioners (which includes the Investigatory Powers Commissioner), and the Investigatory Powers Tribunal. The Independent Reviewer of Terrorism Legislation also reviews security and intelligence agencies from a legislative perspective.

Secretary of State for the Home Department (Home Secretary)

The Secretary of State for the Home Department, also known as the Home Secretary, is the highest political accountability authority for the MI5 and other UK NSI agencies, including the Government Communications Headquarters (GCHQ), and the Secret Intelligence Service (MI6 or SIS) (*Security Service Act 1989*, subsection 1(1); *Intelligence Services Act 1994*, subsections 1(1), 3(1); National Archives of the United Kingdom [UK], n.d., p. 6). The Home Secretary is responsible for all activities of entities encompassed by the Home Office, similar to how Canadian Cabinet Ministers are responsible for their portfolios (Government of the United Kingdom [Government of the UK], n.d.).

In the UK, the responsible Minister is to be held accountable to Parliament through different mechanisms that allow Parliament to question or investigate activities conducted by agencies or departments within the responsible Minister's portfolio. One way parliamentary scrutiny is achieved is by Ministers answering questions about their policy portfolio, and on the departments and agencies within they are administratively accountable for. However, Ministers cannot be questioned about certain issues, including historical events (meaning events that occurred 30 or more years in the past), operational activities that are not decided at the level of the Minister, and legal interpretation (Parliament of the United Kingdom [Parliament of the UK], n.d.).

The Home Secretary's primary mandate is protecting the security and safety of the UK from internal and external threats, including terrorism and crime (National Archives of the United Kingdom [UK], n.d., p. 6). In regard to certain intrusive activities being conducted by MI5, the Home Secretary must authorize warrants (as established in the *Intelligence Services Act 1994*) that either intercept communications or allow MI5 to conduct intrusive surveillance (Security Service, n.d).

Joint Intelligence Committee

While the Home Secretary is accountable for the NSI agencies in the UK, the heads of the three intelligence agencies also have a role in supporting the accountability framework. They comprise

the Joint Intelligence Committee, based in the UK Cabinet Office, along with the heads of military intelligence (Forcese, Roach & Sherriff, 2015, p. 15). They are also invited to attend meetings of the National Security Council, when discussions relate to their legislative purview (Government of the UK, n.d.a). Having a collective decision-making entity such as the Joint Intelligence Committee is thought to have contributed to the UK's success in working with the intelligence agencies of different countries on counter-terrorism, a challenge that "more compartmentalized intelligence and police structures" (Forcese, Roach & Sherriff, 2015, p. 15) have been unable to achieve.

Intelligence and Security Committee of Parliament

The role of Parliamentary review for the NSI agencies is conducted by the Intelligence and Security Committee of Parliament (ISC). Established in 1994 by the *Intelligence Services Act 1994*, the ISC reviews activities conducted the NSI agencies in the UK, as well as the "policies, expenditure, administration and operations of [MI5]" (Intelligence and Security Committee of Parliament [ISC], 2013). The ISC is responsible for providing classified reports, including a general annual report and any special reports to the Prime Minister, and then making an unclassified version available to the public (ISC, 2013).

Investigatory Powers Commissioner

The Investigatory Powers Commissioner's role in providing accountability for NSI agencies is primarily to review warrants issued for MI5 activities involving surveillance, interception, and equipment interference (Investigatory Powers Commissioner's Office [IPCO], 2018). However, they can also be directed to review aspects of intelligence service functions by the Prime Minister (Investigatory Powers Act 2016, subsection 230(1)). All appointed Judicial Commissioners, including the Investigatory Powers Commissioner, must have held or be currently holding high judicial office (Government of the UK, 2018, p. 66).

The creation of the Investigatory Powers Commissioner in September 2017 consolidated three investigative roles previously held by the Interception of Communications Commissioner, the Intelligence Services Commissioner, and the Surveillance Commissioners (Investigatory Powers Commissioner's Office [IPCO], 2018; Government of the United Kingdom [Government of the UK], 2018, p. 57). Prior to this, the above commissioners were responsible for the review of different warrants for intrusive activities conducted by the security and intelligence agencies. Each commissioner was responsible for providing an annual report to the Prime Minister on the activities conducted during the previous calendar year, and an unclassified version of these reports was published for the public to view (Government of the UK, 2018, p. 59).

The authorities of the Investigatory Powers Commissioner have legislative limits to ensure that the Commissioner cannot interfere in either the success of an operation conducted by security intelligence agencies or the effectiveness of the security and intelligence services in the completion of their mandates (*Investigatory Powers Act 2016*, subsection 229(7)).

Investigatory Powers Tribunal

In 2000, the Investigatory Powers Tribunal (IPT) was first established as the independent judicial entity responsible for providing individuals a forum for seeking redress or file complaints against the UK security intelligence agencies, law enforcement and other local authorities (Investigatory Powers Tribunal [IPT], 2016). The IPT's classification as an independent judicial body ensures that it is legislatively protected from government interference during the course of any complaint investigation and when a decision is made by the IPT (IPT, 2016).

Independent Reviewer of Terrorism Legislation

The primary focus of the Independent Reviewer of Terrorism Legislation is to review the fairness, effectiveness and proportionality of legislation related to terrorism (Government of the United Kingdom [Government of the UK], 2018, p. 56). The Reviewer has access to highly sensitive information and the officials who work in counterterrorism and incorporates transparency through producing an annual public report (Government of the UK, 2018, p. 56). The annual report is available to the public, which allows the public to hold NSI agencies to account.

Conclusion

While nations around the world have attempted to create the best structure to hold NSI agencies to account, a variety of factors present implementation issues for those countries seeking to emulate what others have established. This includes the governance structure and who stands as the ultimate overseer of an NSI agency, as what works in one nation may not work in another. However, there is much to be learned from other accountability models based on what types of review and oversight are incorporated into their respective accountability frameworks, and whether any new and potentially innovative mechanisms could stand as an option for other countries to consider in light of evolving threats to Canada and the world writ large.

6. FINDINGS: CANADA'S EVOLVING THREAT ENVIRONMENT

With an increasing level of information injected into the public sphere about CSIS, accountability has become a prominent element of discussions on its role as an NSI agency. To fully understand why the accountability framework for CSIS operates the way that it does, and how this has been impacted by the evolution of the framework, requires a comprehension of the ever-changing global and Canadian threat environments. CSIS's accountability framework must adapt to new contexts. Canada's evolving threat environment, and the changes in how CSIS is able to respond and fulfill its mandate, should have a direct impact on how effective the accountability framework is for CSIS. Changes to the threat environment have also led to increased scrutiny of the overall national security accountability framework in Canada, particularly when it comes to how NSI agencies balance their mandate with accountability and privacy concerns (Littlewood, HillTimes, 2011).

The *CSIS Act* provides CSIS with a mandate to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" (subsection 12(1)). This mandate has shaped CSIS from its establishment in 1984. The *CSIS Act* goes on to clarify the measures CSIS can take to fulfill this mandate, as well as the limitations to these activities. However, to better understand what threats CSIS is allowed to investigate, the *CSIS Act* provides a definition: "a threat to the security of Canada means:

> (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
>
> (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
>
> (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and,
>
> (d) activities directed towards undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada."
> (CSIS Act, 1985, section 2).

In 1981, it would have been difficult for the McDonald Commission to predict exactly what the threat environment would become over time. The combination of the Air India bombing in 1985 and the collapse of the Soviet Union in 1991 marked the end of the context shaping the original CSIS accountability framework and ushered in a new era of security threats that CSIS would need to assess and investigate. The McDonald Commission (1981) noted three primary national security threats to Canada, all of which remain relevant for today (p. 414): first, the activities undertaken by foreign intelligence services, including intelligence agencies from Communist and Middle Eastern nations, and current Canadian allies and partners; second, the promotion of foreign national interests in Canada, and the threat posed to Canadian sovereignty; and third, the

growth of communications and transportation technologies that led to an increased dissemination of terrorist ideologies and the ability to develop an expansive, global terrorist network (McDonald, 1981, pp. 414-415). These threats continue to this day (as demonstrated by the definition in the *CSIS Act*), and, while the specifics may have changed, the foundation of these threats remains the same.

National security threats to Canada in the early 1980s were complex and multi-faceted, which continues to be the case thirty-five years later. The dimension and complexities of these threats have continued to be influenced by increasing globalization, as well as influenced by Canada's NSI partners (Littlewood, HillTimes, 2011). This evolution has had significant implications on whether the CSIS accountability framework can operate at its fullest potential. Evolving threats required the accountability framework for CSIS to evolve with them, taking into account past challenges and their solutions, and future challenges on the horizon (Narrative inquiry, 2019). Globalization drives the need for an accountability framework and defines the scope of national security issues Canada has faced over time and will likely continue to face.

Following the McDonald Commission, events conducted or planned by terrorists were of great concern to Canada's national security. Three major events drew attention to these threats: the attack on the Turkish Embassy in Ottawa on March 12, 1985; the planned threat to bomb the transit system in Toronto in early April 1985 (SIRC Annual Report, 1984-85, p. 13); and the Air India bombings in June 1985, still the deadliest terrorist attack carried out on Canadian soil (Public Safety Canada, 2019, p. 8). The Air India Bombing was a visible demonstration that the threat environment in Canada was shifting away from Cold War dynamics towards a more globalized threat with less distinguishable actors. The CSIS reaction to these events is detailed in a series of government reports, including SIRC's subsequent annual report and the government inquiry into the events and actions leading up to the bombing and actions taken in the aftermath.

The credibility of CSIS's accountability framework was also challenged by the Heritage Front Affair. The Heritage Front Affair was first reported by Canadian news organizations in 1994, with allegations against a CSIS source named Grant Bristow, who had allegedly played an integral role in the foundation of a neo-Nazi organization called Heritage Front and "participated in racist and potentially violent" activities (Whitaker, 1996, p. 279). It was further alleged that Bristow had infiltrated a Canadian political party known as the Reform Party of Canada, spied on the national postal workers union and the Canadian Broadcasting Corporation (CBC), and that a previous federal government administration had used CSIS as a tool to further "its own partisan political goals" (Whitaker, 1996, p. 279). Following these allegations, SIRC, the Inspector General, and a Parliamentary subcommittee on national security conducted investigations into CSIS activities (Whitaker, 1996, p. 280). Because the Heritage Front affair played out in a very public fashion, the public and other stakeholders question the effectiveness of the accountability framework for CSIS (Whitaker, 1996, p. 281). Public questioning of the framework brought different challenges when addressing the perception of the level of credibility for the entities charged with holding CSIS accountable, including the effectiveness of each entity in fulfilling their legislative mandates and how a lack of resources may be contributing to certain inefficiencies.

The terrorist attacks in the USA on September 11, 2001 permanently altered the NSI landscape for Canada. The new *Anti-terrorism Act, 2001* passed that December described terrorism as acts that "constitute a substantial threat to both domestic and international peace and security" and that the Government committed "to taking comprehensive measures to protect Canadians against terrorist activity while continuing to respect and promote the values reflected in, and the rights and freedoms guaranteed by, the *Canadian Charter of Rights and Freedoms*" (*Anti-terrorism Act, 2001*, Preamble). Canada's NSI relationships with other allied nations, including the Five Eyes alliance, became paramount in the years following these attacks. Both the importance of these international relationships and the identification of internal gaps are highlighted through different government inquiries, including the 2006 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (known either as the Maher Arar Inquiry or the O'Connor Commission). The Maher Arar Inquiry noted that inter-departmental cooperation was increasingly required to effectively prevent or respond to threats, and that gaps in co-operation and information sharing between Canadian departments and agencies led to certain failures in protecting the rights and freedoms of Canadian citizens abroad in the period of time immediately following the attacks on 9/11 (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar [Maher Arar Inquiry], 2006, p. 319).

The Edward Snowden revelations in 2013 also altered how many Canadians view national security and NSI activities. While the majority of information released by Snowden highlighted activities of the USA's NSI services, particularly those of the National Security Agency (NSA), Canada was implicated in the released documents as one of its primary intelligence-sharing partners. The revelations led to legislative changes in many countries (such as the *Investigatory Powers Act, 2016* in the UK, and the *Freedom Act, 2015* in the USA) that more clearly detailed what activities such agencies could and could not undertake (MacAskill & Hern, 2018). The documents detailing Canada's role in the mass surveillance network in the USA again focused the Canadian public into discussing the appropriate balance between respecting privacy and ensuring Canada is a safe and secure nation (Canadian Civil Liberties Association, 2019). An Angus Reid Global Survey from October 2013 claimed that as many as "seven in 10 Canadians support Snowden" (CBC News, 2014). Three years later, the 2016 National Security Consultations conducted by the government found that the public was as concerned about NSI agencies as it had been in the early 1980s (Government of Canada, 2017a).

October 2014 marked a visible, tangible indication that Canada was not immune to the national security threats experienced by other countries. In 2014, there were nearly 17,000 attacks worldwide, including the first two terrorist attacks to occur in the capital of Canada (Hill, 2018, p. 18). The image of Canada under threat was elevated because the attacks occurred only a few minutes away from where Canada's parliamentarians and highest-ranking officials regularly convene. These events raised the National Terrorist Threat Level to Medium, which indicates that there is an intent and capability for individuals or groups to carry out an act of terrorism in Canada (Public Safety and Emergency Preparedness Canada [Public Safety Canada], 2019, p. 6). In the years after the attacks in 2014, the national threat level has remained at Medium.

Following the events of 2014, a new Bill, known as the *Anti-terrorism Act, 2015*, received Royal Assent in 2015, expanding the scope of CSIS capabilities. The authorities provided to CSIS under this Act raised concerns about the accountability of CSIS and other members of the NSI

community. The Canadian Civil Liberties Association (CCLA) expressed concerns about the lack of a clear distinction between CSIS and the RCMP and new accountability mechanisms to accompany the expansion of powers for the NSI community (Canadian Civil Liberties Association [CCLA], 2019).

Terrorism itself has evolved from its original definition in the late 20th century, with terrorism shifting towards increased use of unsophisticated tactics, which require minimal resources but cause significant harm to Canadians (Public Safety Canada, 2019, p. 15). Since 2014, Canada has been subjected to an increased number of threats and, while many planned attacks have been prevented, others were successful, including vehicles driven into public arenas and striking pedestrians (such as in Edmonton in 2016 and Toronto in 2018) (Public Safety Canada, 2019, p. 7). Additional threats to national security include Canadian citizens who have travelled to participate in extremist activities abroad and then sought to return to Canada (i.e. Canadian Extremist Travellers), and a rise in right-wing extremism (Public Safety Canada, 2019, p. 10).

Similarly, right-wing extremist attacks in Canada are typically "sporadic and opportunistic" and appear to be domestic in origin (Public Safety Canada, 2019, p. 8). Right-wing extremists are concerned with a wide range of issues but are differentiated from other terrorist groups due to their focus on exploiting an individual's hatred or fear of a particular issue to the point where they act violently (Public Safety Canada, 2019, p. 8). For example, after the 2018 attack in Toronto, where a man drove a vehicle into a crowd of pedestrians and killed 10 people, information found online indicated the attack was driven by the man's hatred of women and their alleged participation in his being "involuntarily celibate", or an "Incel" (Public Safety Canada, 2019, p. 8).

Since 1984, the largest key factor contributing to the evolving Canadian threat environment, and how national security agencies like CSIS respond to potential threats, has been the advancement of technology and how government departments and agencies respond and prevent terrorist events (Public Safety Canada, 2019, p. 28). The McDonald Commission noted the importance of technology and how the rise in globalization could lead to an evolving threat environment for terrorism in 1981, observations since borne out (McDonald, 1981, p. 415). Understanding how threats can generate and spread online is one element that needs to be considered when trying to prevent potential threats from turning into actual attacks on Canada and Canadians. The threat of cyber terrorism was noted by the USA as recently as 2019 as a threat to be monitored, along with new emerging global alliances (e.g. China and Russia), increased global migration, transnational organized crime, the development and consequential application of new technologies, online influence activities (e.g. election interference), and weapons of mass destruction (particularly chemical and biological weapons) and their proliferation (Coats, 2019, pp. 4-8).

Conclusion

The evolution of threats from where they were when CSIS was originally created in 1984 suggests there must be a coinciding change in how CSIS responds to these threats, while ensuring that the steps taken to ensure the protection of Canadians and Canada are necessary and within the rule of law. As the threat environment changes, so must the accountability framework for CSIS in order to both address new threats and to ensure that responses to these threats are

subject to the same review and oversight as other activities conducted under the mandate. However, there are certain challenges to this, as detailed by the findings in the next section.

7. FINDINGS: NSI ACCOUNTABILITY CHALLENGES AND CONTEXT

The effectiveness of the CSIS accountability framework is challenged by issues specific to national security. Much of the available information on this subject looks at different challenges to ensuring effective accountability for Canada's NSI agencies, including the balance between access to information and the necessity for secrecy, adapting to an evolving threat environment, the incorporation of transparency into government practice, and the independence of reviewers. All of these challenges have been present since the inception of CSIS, some more visibly than others, and in some cases, these challenges have resulted in changes to CSIS and to the accountability framework. However, many of the challenges continue persist, though taking new forms and combinations for CSIS. This section explores several themes: secrecy of information, access to information, an evolving threat environment, transparency, and others.

Secrecy of Information

One of the most fundamental challenges that a NSI accountability framework must address is the balance between the use of intrusive investigative techniques in order to preserve the security of the nation, and protecting the rights and freedoms of Canadians, as laid out in the *Canadian Charter of Rights and Freedoms* (Whitaker, 1996, p. 285). With the growth of technology and permeation of information via the Internet in the years since 1984, the importance of striking this balance has only grown in significance. However, NSI agencies like CSIS face challenges in being fully transparent when disclosing information about their activities to the public. Revealing certain information can expose information about targets or investigations and even prevent CSIS from carrying out their mandate in protecting Canadians from threats to their security.

This challenge is not unique to Canada, nor did it start in 1984 with CSIS. Historically, most countries have not shared information about national security and intelligence with the public. The shift towards providing the public and even other areas of government with information about NSI began in Canada with the McDonald Commission and resulted in one of the first pieces of legislation for an NSI agency in Western democracies. Other countries, including the UK and the USA, would eventually follow suit, but Canada led its traditional allies for being one of the first nations in the world to do so.

Conventional belief holds that intelligence is not discussed in public because of the potential danger it could cause to the nation (Farson, 2000, p. 227). SIRC noted in 1986 that information, such as information SIRC includes in their annual reports, could be portrayed ambiguously or even concealed because of its nexus to national security, with the presumption that information in this area is likely classified (SIRC, 1986, p. 3). Rankin (1986) argued that national security often requires a trade-off between the government and the citizens it is responsible for protecting, and that to maintain national security, "a portion of their liberty" (p. 251) would need to be sacrificed to ensure their own personal security in the nation. Rempel (2004) disagreed with the notion that this exchange was absolutely necessary, stating that authorities granted to CSIS should not be allowed to "compromise the civil liberties of Canadians" (p. 636).

This exchange of certain liberties for protection is one not uncommon in Western democracies. A central concern surrounding this trade off was that the government would see an opportunity

to use this convention to justify keeping certain government actions secret from the public, including any "errors, corruption, incompetence, or other inadequacies" (Rankin, 1986, p. 252). Incorporating external and internal review and oversight mechanisms in the CSIS accountability framework was intended to prevent such cover-ups from occurring. However, due to the essential need to keep certain information secret from the public and, in certain cases from the review entities, there may always be a degree of mistrust in the government that remains regardless of how thorough the framework is or becomes.

This information and operational secrecy has led to some public mistrust of NSI agencies and departments, confirmed during the National Security Consultations in 2016 (Government of Canada, 2017a, p. 7). Of the issues captured in these consultations, accountability of the activities conducted by the Canadian NSI apparatus proved to be a central theme in the responses from Canadians (Government of Canada, 2017a, p. 4). The consultations illuminated the importance of review mechanisms, such as SIRC, to prevent unnecessary, excessive or unlawful intrusions into the privacy of Canadians and prevent agencies like CSIS from conducting their operations without additional checks and balances (Government of Canada, 2017a, p. 4). The same consultations also revealed many respondents felt the original safeguards built into the accountability framework for CSIS were not sufficient enough and required enhancement, particularly with regards to oversight (Government of Canada, 2017a, p. 7). However, feedback varied in how review and oversight should occur, particularly whether review should be conducted by a government agency or by an external, independent entity, whether oversight capabilities should be increased, or if oversight by these entities, whether by a government agency or an external body, could ever conduct oversight sufficiently enough to be satisfactory for the public (Government of Canada, 2017a, pp. 4-5).

Access to Information

Since 1984, there has been a changing perception of public access to NSI information, including the degree to which the NSI community itself discussed these matters in a public forum. This represents a steady shift since the McDonald Commission for members of the public and those in the Canadian NSI community. The change in perspective related to the growing access to information was perhaps best summarized by the Director of CSIS in 2013, who said the following in a speech: "It used to be the intelligence community would rarely – if ever – speak to [NSI] issues in a public forum. In today's world, however, it may be that the first line of defence in protecting national security is public awareness of the threat environment." (Government of Canada, 2013, p. 3).

With the increased discussion of the activities conducted by CSIS and other NSI agencies (in Canada and in other nations) comes an increased level of scrutiny from the public. These discussions are still challenged by the fact that CSIS and the NSI community does not, and in many cases cannot, disclose the full extent of its activities and operations without otherwise jeopardizing ongoing operations or sources. As a result, these activities continue to draw concerns from Canadians; particularly about the extent of limitations CSIS must follow when addressing potential threats, and how this is balanced with the rights and freedoms Canadians are legally entitled to under the *Canadian Charter of Rights and Freedoms*.

Of these rights and freedoms, maintaining privacy is one the largest concerns held by Canadians (Government of Canada, 2017a, p. 4). Blais (1989) noted that public satisfaction that their rights are being upheld could be assured through providing clarity to the statutory mandate for CSIS, implementing judicial controls for any intrusive activities CSIS partakes in, and ensuring there is an "arm's length… public reporting function, independent of the executive" (pp. 110-111). Privacy has been prevalent concern for Canadians since 1984 when CSIS was created and has notably continued to be a concern to this day, despite the incorporation of measures to address these concerns. For example, certain activities under the CSIS mandate that will intrude on the privacy of Canadian citizens, such as wiretapping, require judicial authorization through the Federal Court warrant process (SIRC, 1986, p. 2).

During the 2016 consultations, several respondents expressed concern regarding the degree of access to NSI information; more specifically, that SIRC and other review and oversight entities for CSIS lacked the ability or mandate to access all necessary information that would keep CSIS fully accountable for their actions. The information that presented the most concern to the public was the lack of access to information marked as Cabinet confidence. SIRC noted this lack of access as a challenge in their first annual report, discussing it as a challenge that would also impact their ability to comprehensively understand the organizational and operational context that CSIS acted within (SIRC, 1985, p. 13). Because SIRC (and now NSIRA) have a statutory scope of information they are able to review and how they are able to access this information, this continues to make understanding CSIS on a more in-depth level challenging for review entities.

Members of the public, including Murray Rankin, now Chair of NSIRA, criticized this when CSIS was created, claiming the limited scope of access would impact the effectiveness of reviews conducted by SIRC and render the review entity ineffective in the carrying out its mandate. In 1986, Rankin noted that no one entity in the accountability framework, except CSIS itself, could access Cabinet documents, even if it was believed the records would be necessary to the review or oversight being conducted (p. 260). Allowing the agency under review maintain sole access to this information called into question the effectiveness of the reviews conducted by SIRC and others, including the Inspector General. The rationale for this was hotly contested even when the *CSIS Act* was first debated in the House of Commons (Gill, 1989, p. 565). Ultimately, records with Cabinet confidence information were excluded for the possibility of threatening the Cabinet system and the collective responsibility of Cabinet Ministers, but the debate highlighted that, in the past, governments wanted to avoid knowledge of activities that could cause embarrassment (Gill, 1989, p. 565).

The practice of excluding Cabinet records or records containing Cabinet confidence continues to be part of the current framework for review and oversight agencies, including the NSICOP and NSIRA. Concerns persist about possibly increasing the amount of risk for infringement of Canadian rights and continues to be raised by members of the public (Forcese & Roach, 2015, p. 364). Following the tabling of the *National Security Act, 2017*, concerns expressed by civil society groups revealed a belief that the Act would not go far enough in resolving these issues created by its predecessor, the *Anti-terrorism Act, 2015*, and that it created new issues, such as empowering the NSI community to conduct mass surveillance activities without the appropriate level of oversight and ability to stop these activities (CCLA, 2018). However, with new changes

to the framework being implemented at the time of writing, it is possible that some of these concerns may be alleviated, as the new review bodies responsible for CSIS will should gain a better understanding of the broader NSI context by reviews of the entire NSI community.

Adapting to an Evolving Threat Environment

The original CSIS accountability framework and creation of SIRC was considered to be a model for NSI accountability (Forcese & Roach, 2015, p. 423). Experts and academics in the initial years found that the accountability framework was effective in ensuring CSIS was held accountable (Gill, 1989). However, it has tried unsuccessfully to maintain this status, as a result of increasing powers for CSIS and a lack of corresponding changes to accountability mechanisms (Forcese & Roach, 2015, p. 423). One reason for increasing CSIS's capabilities was to better respond to the evolving threat environment. These adaptations to CSIS's operational mandate often correlated with major events or emerging threats to Canada's national security. Unfortunately, as years passed and the accountability framework remained unchanged, the credibility of the methods for holding CSIS accountable diminished.

Several mechanisms help CSIS be accountable in the changing threat environment. SIRC regularly conducted reviews of CSIS activities, including activities related to new threats to Canadians, which were detailed in annual reports. In certain cases, SIRC revisited previous reviews to more effectively assess whether the activities were matched appropriately to the new or developing threat (SIRC, 2014, p. 17). However, this did not always lead to visible or even legislative change, which has led to calls for change by the public. In a letter published by the Globe and Mail in February 2015, 22 Canadians, ranging from former Supreme Court of Canada justices to former SIRC members to former Ministers, called for improvements to Canada's accountability framework to meet the changing environment, as "national security agencies continue to become increasingly integrated, international information sharing remains commonplace and as the powers of law enforcement and intelligence agencies continue to expand with new legislation" (Chretien, J., Clark, J., Martin, P., Turner, J. et al., 2015). The threat environment is unlikely to stop changing in the near future, so reviewing how the accountability framework can continue to hold CSIS effectively accountable should never be far from the scope of the entities conducting review and oversight.

Transparency

While elements of national security require secrecy to ensure the security and protection of Canadians, the public and actors inside government have called for more transparency in national security activities conducted by NSI agencies. With the CSIS accountability framework, transparency occurs on two fronts: between the agency and the review entity, and between the agency and the Canadian public. While academics and critics understand that some secrecy is warranted to protect the security of the country, the degree of transparency between the NSI agency and the review entity must be as complete as possible (Forcese & Roach, 2016, p. 8). The benefits for increasing transparency go both ways: for the review entity, it develops more trust with the agency under reviewed and increases the chances their recommendations will lead to change (Forcese & Roach, 2016, p. 8). For the agency being reviewed, it assists in building up the reviewing entity's confidence in the agency being reviewed.

Transparency with external stakeholders is also being reformed internally to government. The 2017 *National Security Transparency Commitment* is an example of a government-led initiative to broaden the public's understanding of the role and activities conducted by the NSI community and how the NSI agencies can act to increase transparency. The three categories of transparency principles in the 2017 *National Security Transparency Commitment* – information transparency, executive transparency, and policy transparency – demonstrate publicly there are opportunities for enhanced transparency across government (Government of Canada, 2017b).

Public reporting by CSIS and other entities in the accountability framework is another mechanism for transparency, providing the public with another means of understanding how accountability proceeds for NSI agencies. Since 1992, CSIS has regularly published public reports, detailing at an unclassified level the activities and operations undertaken in fulfilling its legislated mandate. This is not a legislative requirement, but following the five-year review in 1989, the government committed to providing the public with more information on national security and the threat environment (Rosen, 2000). Both the Director of CSIS and the Minister continue to fulfill this commitment, first with the Director regularly tabling an unclassified report with Parliament (the most recent report was tabled in June 2019), and second with the Minister providing the public with a report on current threats to further understanding of NSI issues (Public Safety Canada, 2016, p. 1).

Additional Challenges

To ensure CSIS is effectively held accountable, critics and experts in NSI accountability believe it is imperative for review entities to maintain appropriate distance and independence from the government and the agencies they review (Forcese & Roach, 2016, p. 6). SIRC was created to be a non-partisan entity, despite its members being representative of the major parties in the House of Commons (Blais, 1989, p. 114). In its 1985-86 Annual Report , SIRC (1986) explicitly states the methods taken to remain independent of Parliament, including keeping "an arm's-length relationship with [CSIS] and other direct participants in the Canadian security intelligence establishment… [and] consciously avoided becoming part of the system and giving the appearance of being 'insiders'" (p. 3). In their paper on the ideal accountability framework for CSIS and other Canadian NSI agencies, Forcese and Roach (2016) argue that independence of the review entity from the government and the agency being reviewed prevents the perception of the review entity being "beholden to the government" (p. 7). Independence is not a recent consideration for effective accountability of CSIS. The idea of maintaining independence from the government and CSIS influenced the development of the structure for SIRC in the first place.

Concerns about when oversight and review should be conducted in the course of an operational timeline were raised during the legislatively mandated five-year review of CSIS (Blais, 1989, p. 115). One concern was the potential for negatively impacting the behaviour of operational CSIS officers, causing them to act defensively or be hindered by an unnecessary degree of caution (Blais, 1989, p. 115).

Among the other concerns raised by academics and independent reviews, coordination among departments and agencies responsible for protecting the safety and security of Canadians was the

most common to be brought up in literature. Coordination, as argued throughout the Maher Arar Inquiry, was and clearly remains a significant factor in successfully preventing and responding to threats (2006). There will always be areas where coordination can be improved, even with the changes brought in with the *National Security Act, 2017* in 2019. For example, there is no well-defined entity solely responsible for identifying, analyzing or reporting on threats emerging across the different NSI agencies (Leuprecht & McNorton, 2018, p. 6).

Conclusion

The challenges to ensuring CSIS is held accountable are not new to national security, nor are they new to Canada. One of the largest challenges for holding CSIS accountable is the necessity for the secrecy of certain information, which consequently also limits the ability for those outside of the NSI community to gain access to information. However, over the last thirty-five years, the culture of information transparency and overall threat environment have changed significantly, especially with regard to the public's role in accountability and overall access to information that the public expects from the government.

8. DISCUSSION AND ANALYSIS

The remainder of this paper will focus on analyzing the above findings, before presenting three policy options and a recommendation for consideration by Public Safety Canada. In this section, the analysis begins by first presenting an overarching summary of the findings and a discussion of the cross-cutting themes that emerged through these sections. This will include an updated version of the original CSIS accountability framework to illustrate the changes to the overall organizational structure of the framework in 2012 and 2019, as well as a revised analytical framework to demonstrate how the changes between 1984 and 2019 have impacted the accountability process. The section will conclude with an examination of the implications these findings have on the policy options.

Summary of Findings

In 1984, Canada was the first among its allies to establish an accountability framework for its NSI agencies. This framework was considered at the time as being one of the most comprehensive for NSI agencies, as it incorporated multiple mechanisms spread through the three branches of government in a collaborative approach to ensure the following: first, that CSIS could be held accountable for all activities conducted, both before and after they occurred; and second, to demonstrate both internally and externally how the new NSI agency was being held accountable through increasing transparency between CSIS and the entities within the framework, as well as between CSIS and the Canadian public. As time has passed other nations throughout the global NSI community have established their own frameworks, which recent literature suggests has, in some ways, surpassed the CSIS framework in its ability to effectively hold the agency accountable.

In order to effectively meet the evolving threat environment and protect the security and safety of Canadians, CSIS has been granted certain powers and authorities over the last thirty-five years that were not in the original *CSIS Act*. However, the expansion of operational capabilities for CSIS were not met with any corresponding changes to the entities responsible for holding them accountable until 2017.

Since the establishment of CSIS, the ability of the review entities to hold CSIS accountable has been faced with a series of complex issues, made complex thanks to the NSI context in which CSIS operates. Of those issues, secrecy of information, access to information, and transparency of NSI activities and information have remained most predominant. Since the 2016 National Security Consultations, there has been a gradual move towards transparency of the NSI community. In turn however, this increase in transparency has also contributed to greater scrutiny of the kinds of activities CSIS is conducting on the behalf of Canadians. When it comes to more intrusive activities that have the potential to infringe on rights and freedoms, Canadians have indicated the importance of having an effective framework to hold CSIS accountable.

Since 2017, the government has taken steps to improve the CSIS accountability framework through the establishment of the new parliamentary review body, the NSICOP. As well, the passage of the *National Security Act, 2017* in 2019 has reformed several of the pre-existing accountability mechanisms for CSIS. Despite the scope of reforms to the accountability

framework, the impact is largely expected to be positive, with few negative impacts once the implementation stage has passed and the entities have established their procedures and processes for review (Narrative inquiry, 2019). This expectation is similar to what had been noted by SIRC in the first reports after it was established in 1984.

Conceptual & Analytical Frameworks of CSIS Accountability

To reflect the changes to the accountability framework for CSIS found in Figure 1, two more frameworks have been developed. Figures 3 and 4 capture the changes to the original 1984 accountability framework structure: the first occurring in 2012, following the elimination of the Inspector General; and second in 2019, reflecting the many changes to the accountability structure after the passage of the *National Security Act, 2017*.

FIGURE 3: 2012 Accountability Framework for CSIS

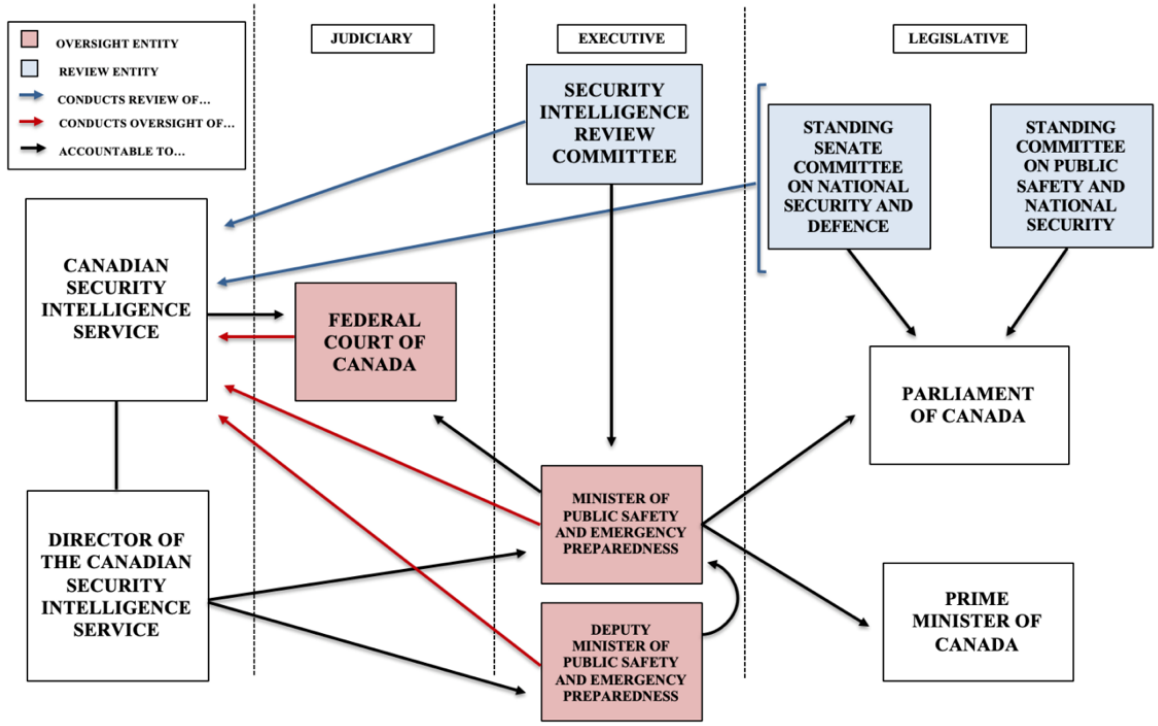
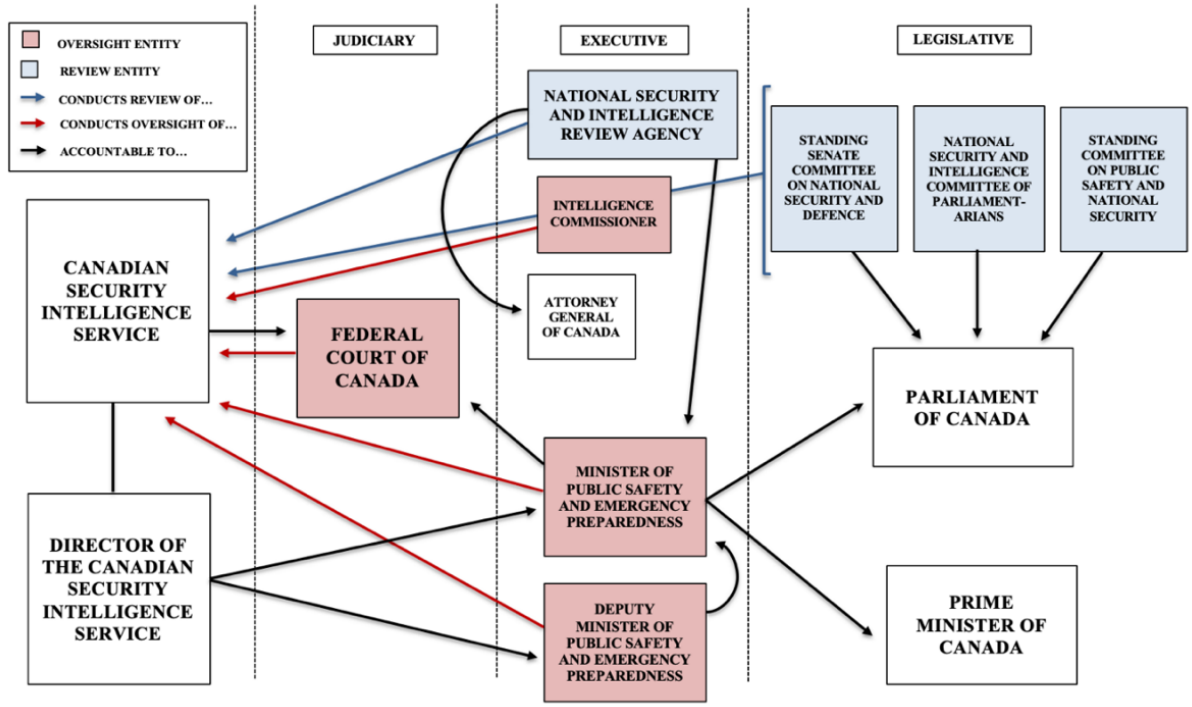


FIGURE 4: 2019 Accountability Framework for CSIS

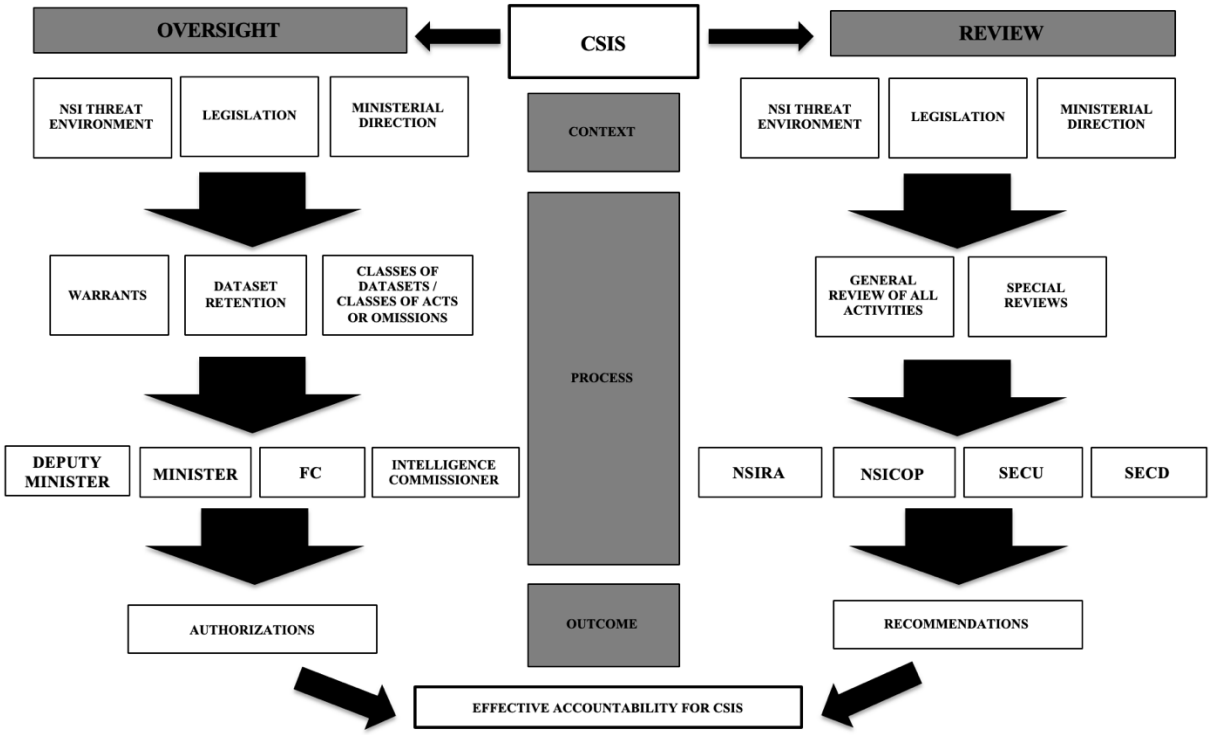


Both frameworks captured in Figures 3 and 4 are considerably more detailed in comparison to the original 1984 accountability framework and appear to demonstrate that the structure for holding CSIS accountable became progressively more complex. The findings suggest that this was primarily the result of two factors:

- First, that the evolving threat environment and the coinciding increase in powers and authorities granted to CSIS in order to fulfill their mandate had not initially been met with increased review capabilities; and,
- Second, that the increased number of departments and agencies within the federal government warranted the establishment of an entity (or entities) capable of conducting review and oversight of the Canadian NSI community as a whole, rather than in siloes.

The increasing complexity of the accountability framework for CSIS raises the question of whether a more intricate and complex structure is the most effective way to holding CSIS accountable or whether a more streamlined system of checks and balances is more effective (Narrative inquiry, 2019). To demonstrate how the accountability framework functions in practice, Figure 5 (see next page) breaks down this process in detail using an analytical framework. This was first demonstrated in Figure 2, showing what the process looked like in 1984 when CSIS was first established. Figure 5 illustrates what accountability processes are in place as of 2019, thirty-five years later. The analytical framework begins with the context and parameters in which CSIS operates, then establishes the process for conducting review and oversight and by whom, and concludes with the outcomes of each process.

FIGURE 5: 2019 Analytical Framework for CSIS Accountability



The importance of the responsible Minister for CSIS is clearly evident in Figures 2 and 5. Since the framework was first established, the importance role of the Minister in conducting oversight has been recognized, as one of the elements of the framework left unchanged over thirty-five years. But, as Figures 1-5 only focus on CSIS and not the other departments and agencies within the Minister's portfolio, the frameworks do not reflect the significant expansion of the portfolio since 1984, which has led to challenges for the Minister and their ability to be informed of CSIS activities.

Cross-Cutting Themes from Findings

Implementation of Accountability: Policy in Practice

There has never been any doubt about the importance of ensuring a structure of accountability for a Canadian NSI agency like CSIS; however, questions have persisted about the most effective level of accountability that should be enacted. From the outset of the creation of CSIS, the federal government has placed specific emphasis and importance on having multiple mechanisms in place to ensure there is accountability for the agency's activities. Each component of the CSIS accountability framework has an important role to play for CSIS. However, as with all policy, putting policy into practice does not always mean that expectations will be met over time (Narrative inquiry, 2019). Operational and administrative realities often mean that the effectiveness of an accountability framework cannot be fully evaluated unless it has been engaged for a period of time. When CSIS was first created, a mechanism for review after five years was placed directly into legislation. This practice was again utilized in the

National Security Act, 2017, though it is after a notably shorter time period, being only three years instead of five, and was again only a one-time review.

This evaluation of the framework's effectiveness is also impacted by the scope of review that is conducted. Prior to 2019, none of the entities in the CSIS accountability framework were responsible for reviewing the Canadian NSI community as a whole. As early as 1986, the idea of having a review entity with this capability would provide the review with a more comprehensive picture of how all of these agencies function together and close any gaps in broader contextual understanding (Rankin, 1986, p. 259). SIRC as well saw the challenges in having an NSI review body with a mandate to review only one aspect of the entire NSI structure, with the first Chairperson of SIRC notably questioning the effectiveness of a review body that was only able to review one segment of the larger NSI community (Gill, 1989, p. 561). Forcese & Roach (2015) also examined this closely and argue that the effectiveness of the review entity like SIRC decreases "when reviewers or overseers do not have adequate powers, information, or resources to match the conduct that is being reviewed" (p. 364). It remains to be seen whether the creation of NSIRA in 2019 will provide the necessary comprehension to CSIS and the NSI community as a whole.

With both the original establishment of the accountability framework and with the changes being made in 2019 to expand the framework itself, there appears to have been an emphasis on ensuring there be a specific purpose for each entity within the accountability framework in order to prevent redundancy or inefficiencies. For example, this can be seen in the structure for how the NSICOP and NSIRA are able to conduct their reviews of the NSI community; the NSICOP is much more restricted in the kinds of information they are allowed to access, which forces their reviews to be more high-level, whereas it is expected that NSIRA, who is allowed to access a greater scope of information, will be able to perform much more detailed reviews of operational activities and policies across the NSI community. However, NSIRA is mandated to conduct certain reviews, including of CSIS and CSE, on an annual basis, as well as reviews of NSI activities specifically noted in legislation (such as an annual review of the application of Governor in Council directions on avoiding complicity in mistreatment by foreign entities by certain departments and agencies). At the time of writing, NSIRA has not published any reports on reviews conducted by the organization, so there are no examples to draw from regarding level of detail or scope of access to information that will be included in their public reports.

International Frameworks and Compliance

The accountability framework for CSIS differs from Canada's traditional allies, particularly with the lack of direct parliamentary oversight of CSIS and other NSI agencies, and a lack of independent monitors, such as the Independent Reviewer of Terrorism Legislation in the UK or the Inspector General of the CIA in the USA. Given the limited role of the new Intelligence Commissioner in examining compliance of specific CSIS activities, it is challenging to compare the role with those in the international models presented in this paper. This brings into question the extent of the role of the judiciary in Canada, as the FC plays a key function in ensuring oversight and compliance of CSIS activities in a manner that is external to the Minister and CSIS itself. In the past, the FC has had a role in pointing to gaps in legislation related to CSIS. However, as the FC only plays a role in the authorization of certain activities and not the day-to-

day operations of CSIS, it can only provide decisions on the activities it is made aware of through the judicial system.

Challenges to NSI Accountability

Overall, the system of accountability for CSIS is still subject to the same challenges that other nations have faced with increased frequency in the previous two decades, such as a changing threat environment and a growing public interest in how NSI agencies conduct themselves on behalf of the nations. One of the findings noted during the course of the narrative inquiry was the fact that the incorporation of more transparent accountability functions was not only central to CSIS from an internal perspective, given their responsibility to maintain accountability and compliance with their legislative mandate, but also from an external perspective (Narrative inquiry, 2019). By having these reviews accessible to the public, this presents an opportunity for CSIS to demonstrate and justify to Canadians that the agency legally utilizes the powers and authorities granted to them by legislation in order to protect Canadians from threats to their security. However, the findings from the narrative inquiry also raised the question of the proportion of review entities to those entities mandated to conduct oversight, and whether the accountability framework would benefit from additional oversight instead of added review (Narrative inquiry, 2019).

Role for Ministerial Oversight

Unlike review, Ministerial oversight of CSIS has remained virtually unchanged since the establishment of the agency in 1984. The institutional nature of Ministerial oversight does not provide much flexibility in changing how this oversight is conducted; in fact, this responsibility for Cabinet Ministers is a requirement for the Minister once an oath of office has been sworn. The purpose for the Minister has always been for the Minister to be ultimately accountable for CSIS, given their established responsibilities as both a Cabinet Minister and as an elected official (Cronk, 1985, p. 2). However, this does not alter the importance of having such a role integrated into the accountability framework for CSIS. Certain decisions are to be made only by the Minister, such as the approval of a warrant application to the FC requesting authorization to conduct certain, limited activities that would be considered intrusive to the individual. In order for them to effectively be held accountable, these decisions cannot be made without being appropriately apprised of as much information as necessary to make the decision to request such activities.

Impact of an Evolving Threat Environment

External variables beyond review have also generated changes to the accountability framework over the last thirty-five years. Part of the challenge in adapting to an evolving threat environment is that the entities charged with holding CSIS accountable are primarily conducting review of past activities and are making recommendations based on information that was prevalent in past decision making (Narrative inquiry, 2019). While this may be sufficient in some circumstances, not all threats can be effectively addressed solely by this reactive process. The legislative mandate of CSIS requires the agency to not only address and react to threats in the present but to also proactively consider what threats may potentially need to be addressed in the future and

determine what steps can be done proactively to prevent such threats from occurring. The Minister, as the expected holder of knowledge, must accordingly adopt this mindset as well, as the Minister not only makes decisions in the present, but must also be forward-looking in their approach to ensuring CSIS is able to effectively fulfil their mandate (Narrative inquiry, 2019). This role highlights the importance of oversight in holding CSIS accountable for both their activities and in ensuring they are able to successfully fulfill their mandate. Additionally, the entities responsible for conducting oversight, such as the Intelligence Commissioner and the FC, do so only in very specific contexts; only the responsible Minister has both the knowledge of the broader nexus and the decision-making authority required to hold CSIS fully to account.

Conclusion: Implications for Developing Policy Options

Many aspects of the accountability framework, particularly with regards to review, have undergone significant changes since 2017. The establishment of NSIRA as the entity responsible for conducting review of all federal government institutions conducting NSI activities, not just CSIS, is expected to positively alter the accountability landscape. The scope of review under NSIRA should contribute to better understanding of how the NSI Community works as a whole to protect the safety and security of Canada, which even SIRC notably admitted that they were unable to fully understand, given their limited review mandate. This will be supplemented by the annual reporting requirements for both the NSICOP and NSIRA, as the public release of the reports allows for the potential of an increased discourse about accountability for CSIS.

With a steadily evolving threat environment, the activities conducted by CSIS have adapted to correspond with new or changing threats to Canada. As identified by the McDonald Commission in 1981, these activities must then be held to account by a framework of review and oversight involving all three branches of government. The ability to review CSIS through the executive and legislative branches of government has led to successive recommendations that CSIS alter procedures and policy to remain compliant with the law and their legislated mandate, while also ensuring CSIS remains effective in protecting the safety and security of Canadians.

The CSIS accountability framework is undergoing significant changes. However, the findings of this paper indicate that given the constantly evolving NSI context in which CSIS is in, there will always be a need to further adapt the accountability framework to meet emerging needs. Given this reality, the next section identifies three policy options to further enhance the CSIS accountability framework and ensure that there continues to be effective, multi-faceted mechanisms in place to ensure CSIS is held to account.

9. POLICY OPTIONS AND RECOMMENDATION

The purpose of this section is to outline opportunities for the further enhancement of the CSIS accountability framework. There are three policy options being proposed, including:

1. Enhance the Role of Deputy Minister in the Accountability Framework
2. Decrease the Size of the Ministerial Portfolio
3. Require Regular Review by the NSICOP of the CSIS Accountability Framework

Each option is based on the findings of this report and were analyzed with respect to possible organizational and political risks that may arise. This section identifies a recommended option and sets out some key considerations on implementation.

Option 1: Enhance the Role of Deputy Minister in the Accountability Framework

Option 1 proposes amending the CSIS Act to increase the mandate for the Deputy Minister of Public Safety (Deputy Minister) in order to increase support to the Minister in holding CSIS accountable. The CSIS accountability framework in 1984 was greatly influenced by the recommendations of the McDonald Commission, which strongly called for oversight of CSIS by the Minister, who must be accountable to the executive and legislative branches (McDonald, 1981, p. 408). To effectively hold CSIS accountable for their activities (e.g. warrants), the Minister is obligated to ensure they are well-informed (Canada: R. v. X (Re), 2017, FC 1048). Since 1984, this recommendation by the McDonald Commission has been further supported and reinforced by other commissions of inquiry, special reports, and FC court decisions.

Ministerial oversight continues a central component in the CSIS accountability framework, and this did not change with the passage of the *National Security Act, 2017* in 2019. While the CSIS accountability framework has undergone significant changes, particularly with establishing NSIRA, and incorporating supplementary oversight from the new Intelligence Commissioner, the role of the Ministerial oversight was largely unaffected. This was also the case for the Deputy Minister, whose role is to support the Minister in carrying out responsibilities under the CSIS accountability framework.

Of the entities encompassed within the accountability framework, including the new Intelligence Commissioner, the Deputy Minister is best positioned to better support the Minister without creating a new entity. The Deputy Minister is already enabled by the *CSIS Act* to provide advice to the Minister on any Ministerial directions that either has or could be issued to CSIS, and the Deputy Minister is required to be consulted by the Director of CSIS on general CSIS operational policies, on Ministerial directions issued by the Minister to CSIS, and on warrant applications prior to being sent to the Minister. Prior to 2012, the Inspector General and the position's monitoring statute provided the Minister with a supporting function in conducting oversight of CSIS. However, eliminating this role and the reallocation of their functions to SIRC and the Minister meant that the Minister was expected to take on new responsibilities, without additional resources. To alleviate some of this burden that the Minister took on, this option proposes to amend the *CSIS Act* to incorporate an enhanced supporting role for the Deputy Minister which avoids creating a new oversight entity and expanding the reformed accountability framework.

Amending the *CSIS Act* to enhance the role of the Deputy Minister addresses certain issues raised in relation to the effectiveness of the Minister in holding CSIS accountable, including:

- The Minister's obligation to be as informed as possible in order to perform their oversight role effectively, while simultaneously fulfilling their responsibilities as the accountable Minister; and,
- The Minister being appropriately supported by different elements of the accountability framework, to ensure sufficient dedicated mechanisms to support them in oversight.

Amending legislation to include more information about the role of the Deputy Minister in supporting the Minister will also serve as a mechanism of transparency. The government committed in the 2017 *National Security Transparency Commitment* to improve transparency of the NSI community with the Canadian public. By enhancing and then incorporating the Deputy Minister's responsibilities in more detail under the *CSIS Act*, the government will continue demonstrating commitment to all three NSI transparency principles.

There are some organizational and political risks to Option 1. A political risk includes the timing of future amendments to the CSIS Act. As the entire CSIS accountability framework underwent significant reform in 2019 and has only been in effect for a few months, there would likely be little interest from implicated parties in revisiting amendments to the CSIS accountability framework so soon. It could make more sense to wait for the implementation of the new accountability structures before making further changes. An organizational risk is related to the removal the role of Inspector General in 2012. Then it was argued the position was no longer needed, which is why this position as one of the Minister's oversight supports was eliminated from the accountability framework. While Option 1 does not create a new entity in this process, enhancing the role of the Deputy Minister raises the question of why additional supports are needed once more. Finally, while not necessarily a risk, legislative amendments are not the only tool available to the Minister in enhancing the Deputy Minister's role in the accountability framework. The Minister could use their authorities under the *Public Safety and Emergency Preparedness Act*, and issue Ministerial directions to the Deputy Minister on this subject, as the Minister did with the 2015 Ministerial Direction on Accountability and Operations.

Option 2: Decrease the Size of the Ministerial Portfolio

Option 2 proposes decreasing the size of the Minister's policy portfolio to improve the Minister's capacity to hold CSIS accountable with the Minister's legislated oversight function, and to be held accountable for the activities undertaken by CSIS with Ministerial authorization. The Minister is now responsible for a large, diverse, and demanding ministerial portfolio, which, given the requirement of the Minister to be as knowledgeable as possible for all departments and agencies, makes being fully and effectively accountable difficult. The mandates of each entity, while varying slightly depending on their context, all have the same overarching expectation: they work to keep Canada and Canadians safe from threats to the security of the nation. The Minister is responsible for ensuring these agencies fulfil this mandate and are held to account in how they do so. The proposed new portfolio for the Minister would include CSIS, the RCMP, CBSA, Public Safety Canada, the Review and Complaints Commission for the RCMP (CRCC), and the External Review Committee, and would require the Correctional Service of Canada, the

Parole Board of Canada, and Office of the Correctional Investigator to be reallocated to a different portfolio.

Prior to 2003, there were only five departments and agencies in the portfolio of the responsible Cabinet minister (which was the Solicitor General at the time) (Privy Council Office, 2001, p. 5). However, sixteen years later in 2019, the Minister is now responsible for six departments and agencies, and three review entities (Public Safety Canada, 2019). The expansion of this portfolio, coinciding with the increase in powers and authorities granted to CSIS, makes it challenging for the Minister to hold each entity in the portfolio fully accountable and in turn for the Minister to be held accountable.

One way to ensure that the Minister is able to effectively maintain this level of accountability of CSIS is to reduce the size of their ministerial portfolio to include only those departments and agencies that directly engage in matters of national security and intelligence, and their respective review bodies that fall under the Minister's purview. By doing so, the Minister would have an increased bandwidth to effectively ensure the accountability of the departments and agencies remaining within their portfolio. This would likely occur in part because of the potential these changes have in alleviating some of the administrative and legislative burdens associated with having a large and complex portfolio.

The reallocation of the three organizations above could also have additional benefits for them, and not just the remaining departments and agencies in the Minister's portfolio. For example, a new Minister could have additional capacity to hold these agencies accountable. As well, a different Minister might have a portfolio better suited to addressing the policies and matters of the three organizations, such as the Minister of Justice and the Attorney General of Canada. The latter Minister has worked closely with the Minister of Public Safety on a range of issues related to these three organizations in the past, including most recently with the *National Security Act, 2017*.

Option 2 has some risks. The largest risk associated is organizational, as decreasing the size of the Minister's portfolio requires multiple changes to the machinery of government. In moving three of the organizations out of the current Minister's portfolio, they would have to be reallocated to the portfolio of another existing Minister or to the portfolio of a new Minister. It would also require legislative changes, including amending existing legislation and potentially creating new legislation. There is also political risk for the Minister in decreasing the size of the portfolio. Narrowing the focus of the portfolio could result in a loss of knowledge and understanding in how all of the elements within the current portfolio function and interface with one another.

Option 3: Require Regular NSICOP Review of the CSIS Accountability Framework

Option 3 proposes to amend the *CSIS Act* to include mechanisms for regular review and reporting every four years on the CSIS accountability framework. This review would be conducted by the NSICOP. The precedent for conducting parliamentary review of CSIS accountability framework is the original 1984 legislation, which included a mandatory review to ensure that the *CSIS Act*, and by extension the accountability framework, were reviewed by a

parliamentary committee. A similar parliamentary review was also incorporated into the *National Security Act, 2017;* however, the review will be of the entire omnibus bill that came into force in 2019 and not just the *CSIS Act*. In 1984, the accountability framework was established directly in the *CSIS Act*. Today, the accountability framework for CSIS is spread out over several pieces of legislation, including the *NSIRA Act*, the *NSICOP Act*, and the *Intelligence Commissioner Act*.

Incorporating regular review of the CSIS accountability framework would inculcate a proactive approach to addressing any issues with the framework and, if necessary or appropriate, amending legislation. Over the last thirty-five years, the *CSIS Act* has been amended infrequently, and generally in response to two events: major events, such as the attacks in the Canadian National Capital Region in October 2014; or key decisions from the FC on CSIS activities, such as the 2016 FC decision on datasets and duty of candour. By establishing regular, proactive review with a parliamentary committee, the *CSIS Act* will more likely to be frequently and proactively updated and demonstrate to the public that the agency is not only reactive, but also looking ahead.

Regular review of the accountability framework is also an opportunity to more frequently evaluate the effectiveness of certain activities or authorities. While NSICOP cannot conduct reviews of other review entities (such as NSIRA), NSICOP reviews of the CSIS accountability framework would still have the added benefit of assessing how CSIS responds to reviews conducted by other entities within the accountability framework. Conducting periodic review would also bring Canada more in line with international allies, including the UK, which established entities (e.g. UK's Independent Reviewer of Terrorism Legislation) to specifically review NSI-related legislation.

The purpose of having the NSICOP, and not NSIRA, as the review entity to conduct regular review of the CSIS accountability framework is two-fold. First, the statutory mandate for NSICOP directly refers to reviewing any "legislative, regulatory, policy, administrative and financial framework for national security and intelligence" (NSICOP Act, section. 8). The CSIS accountability framework could be reviewed based on this mandate. Second, it would bring a different perspective to the review given that all members of the NSICOP must be sitting members of Parliament. The incorporation of regular review and reporting by the NSICOP would seek to increase the level of transparency around the processes of accountability for CSIS.

Option 3 has organizational and political risks. The two big organizational risks associated with implementing Option 3 includes review fatigue for entities within the CSIS accountability framework, and the NSICOP's access to information for conducting their reviews. First, CSIS is already subject to annual review by NSIRA and the NSICOP, and while this review would be specifically assessing the accountability framework, it would still implicate CSIS personnel. Incorporating further elements of review into the accountability framework for CSIS could place additional burden on resources in the existing accountability structure. This burden could negatively impact the ability of organizations, including CSIS and Public Safety Canada, in participating in reviews by multiple entities and fulfilling their mandates due to review fatigue. Second, is that NSICOP is only entitled to review certain information in the course of their reviews. This limited access to information could create challenges in assessing the full extent of

the effectiveness of the accountability framework, and from identifying opportunities for improvement. NSICOP would also be unable to conduct reviews of NSIRA or the Intelligence Commissioner, which would consequently limit their ability to access information from either entity.

The political risk is connected to the second organizational risk. By only reviewing the CSIS accountability framework, and not the broader NSI accountability structure, it is possible that the NSICOP will face the same narrow mandate challenges that SIRC did when conducting their reviews of CSIS. In particular, SIRC was only mandated to review CSIS information and consequently was unable to review information from other departments and agencies that might have been implicated in the information collected from CSIS.

TABLE 4
Summary Comparison of Policy Options

Policy Options	Benefits	Organizational Risk	Political Risk
Option 1: Enhance the Role of Deputy Minister in the Accountability Framework	• Deputy Minister is best positioned to better support the Minister without creating a new entity and avoids creating a new oversight entity or expanding the recently reformed accountability framework. • Addresses certain issues raised in relation to the effectiveness of the Minister in holding CSIS accountable, including: - The Minister's obligation to be as informed as possible in order to perform their oversight role effectively, while simultaneously fulfilling their responsibilities as the accountable Minister; and, - The Minister being appropriately supported by different elements of the accountability framework, to ensure sufficient dedicated mechanisms to support them in oversight • By enhancing and incorporating the Deputy Minister's responsibilities in more detail in the CSIS Act, the government will continue demonstrating its commitment to the *2017 National Security Transparency Commitment.*	• New accountability framework has only in effect for a few months and it is hard to evaluate whether further legislative changes would be needed. • Enhancing the role of the Deputy Minister raises the question of why additional supports are needed, particularly given the rationale behind removing the role of Inspector General in 2012.	• Lack of appetite to make amendments to legislation so soon after the CSIS accountability framework underwent significant reform. • Minister could issue Ministerial Direction to Deputy Minister, as opposed to making legislative amendments.
Option 2: Decrease the Size of the Ministerial Portfolio	• Potential to improve the Minister's capacity to hold CSIS accountable with the Minister's legislated oversight function, and to improve the ability for the Minister to be held accountable for the activities undertaken by CSIS with Ministerial authorization.	• Decreasing the size of the Minister's portfolio requires multiple changes to the machinery of government. • Would require legislative changes, including amending existing legislation and	• Narrowing the focus of the portfolio could result in a loss of knowledge and understanding in how all of the elements within the current portfolio function and interface with one another.

	• Minister would have an increased bandwidth to effectively ensure the accountability of the departments and agencies remaining within their portfolio. • Different or new Minister could have additional capacity to hold these agencies accountable or could have a portfolio better suited to addressing the policies and matters of the three organizations, (e.g. Minister of Justice and the Attorney General of Canada).	potentially creating new legislation if new Ministerial role were created.	
Option 3: Require Regular Review by the NSICOP of the CSIS Accountability Framework	• Regular review of the CSIS accountability framework would inculcate a proactive approach to addressing any issues with the framework (including effectiveness of certain activities or authorities granted to CSIS and how CSIS responds to other entities within the accountability framework) and, if necessary or appropriate, amending legislation. • NSICOP reviews of the CSIS accountability framework would have the added benefit of assessing the effectiveness of new and existing review entities in holding CSIS accountable. • NSICOP, rather than NSIRA, would bring a different perspective to review of the accountability framework by virtue of its parliamentarian-only membership.	• Inclusion of additional review mechanisms has the potential for increasing chance of CSIS and other affected departments/ agencies experiencing review fatigue. • *NSICOP Act* sets limitations to kinds of information the NSICOP can access when conducting reviews. • NSICOP cannot conduct reviews of other entities within the framework (e.g. NSIRA).	• Narrow scope of review could mimic challenges to conducting effective reviews that was faced by SIRC.

Recommendation: Implement Option 1 – Enhancing the Deputy Minister's Role

All three policy options are opportunities to further the effectiveness of the accountability framework for CSIS and were developed as mutually exclusive options. However, Option 1 emphasizes the importance of the role of Ministerial oversight by enhancing an existing aspect of the accountability framework by providing additional support to the Minister with an enhanced Deputy Minister role. This option directly targets gaps in the accountability framework identified in previous reviews. Given the transparency required of the amending legislation, Option 1 would also provide the public with more information to greater understand how the framework works to hold CSIS accountable.

Option 2 also increases effectiveness from an organizational perspective. It could provide the Minister with an increased level of bandwidth to perform their accountability functions. However, Option 2 is not recommended because of the significant restructuring of multiple departments and agencies and the degree of machinery changes that would be required.

Option 3 suggests increasing the capacity for a review body and acknowledges the important role for parliamentary review in the accountability framework. Since NSICOP is responsible for conducting reviews in matters related to national security and intelligence, it could reasonably be considered as a prime vehicle for regularly reviewing CSIS and the *CSIS Act*. However, there is a higher potential for creating review-related burden on CSIS resources and would increase the potential for review fatigue.

Implementation Considerations

There are three primary aspects to implementing Option 1 that must be considered, including:

- The amount of time required for Option 1 to be implemented;
- The level of resources required for both the Deputy Minister and the corresponding review entities (e.g. NSIRA) that would be responsible for conducting review of the enhanced role; and,
- The process for how the accountability process is made transparent, as per the *2017 National Security Transparency Commitment*, following the enhancement of the role for the Deputy Minister.

Given the recent changes to the CSIS accountability framework, it seems unlikely that any legislative enhancement of the Deputy Minister role would be tabled in Parliament for at least one or two cycles of reviews conducted by the new framework. This allows the new review entities to fully establish administrative and procedural processes for reviewing all of the departments and agencies that fall within their mandate scope and could provide further evidence to justify enhancing the Deputy Minister role to increase support for Ministerial oversight. Further, as there have not been any reports from the new review entities (the exception being the 2017-18 Annual Report from the NSICOP), it is challenging to predict what these reports will look like and what the focus of their reviews will be on. Timing of enhancing the Deputy Minister role would also need to be considered in the context of the legislated review of the *National Security Act, 2017*, slated to occur in 2022-23.

Once the timing for these changes has been identified, the level of resources required for both the Deputy Minister and the respective review entities would need to be determined. Increasing responsibilities for these aspects of the CSIS accountability framework would likely require an increase in resources provided to them, in order to ensure that not only is the Deputy Minister is able to effectively support the Minister with their oversight responsibilities for CSIS, but that the review entities are able to access resources to maintain their ability to conduct effective reviews.

The final consideration is the level of transparency between the implicated Government departments and agencies, and the Canadian public. Incorporating changes to the Deputy Minister role in legislation not only provides an enhanced legislative mandate for the Deputy Minister but also serves as a mechanism of publicly demonstrating the process through which CSIS is held accountable. While certain details of CSIS operations and activities cannot be shared with the public, making the process of accountability accessible to the public (e.g. publication of legislation) would assist in maintaining the confidence of Canadians in what CSIS does to protect them and the country as a whole from threats.

10. CONCLUSION

Accountability for CSIS continuously evolves to effectively address changes to the environment it finds itself in. While CSIS's accountability framework is, by admission of the entities within it, not perfect, the unique nature of the NSI context creates additional complexities in holding to account the agencies responsible for keeping Canadians safe and secure from threats. The inclusion of review and oversight entities across multiple branches of government creates a complex and comprehensive structure for ensuring this purpose. Even with the significant restructuring of the entities within the framework over the last eight years, certain institutional elements (e.g. Ministerial oversight) remain the backbone of the accountability framework.

Incorporating Ministerial oversight of CSIS was designed to ensure that this balance would be maintained, as the responsible Minister was both politically and legislatively accountable for the activities conducted by CSIS. This goal has not changed in the decades since the McDonald Commission recommended the creation of an NSI agency outside of the RCMP. However, while the accountability mechanisms delineating the Minister's role have been altered and changed to adapt to an evolving environment, the functions of the responsible Minister for CSIS remain the same as they were in 1984. An expanding scope of the Minister's responsibility does not detract from the fact that the Minister is ultimately responsible and accountable to the Government, to Parliament, and to the public for the activities conducted by CSIS.

Over time the effectiveness of CSIS's accountability framework has been challenged. These challenges, which were not anticipated during its original development, included: SIRC's inability to review NSI activities writ-large due the CSIS-only legislative mandate; the evolving threat environment and the growth of legislated powers and authorities granted to CSIS; and increased pressure from the government and the public to improve transparency of information related to national security. The legislative changes made since 2017 have sought to address many of these issues, and through the recent changes to the accountability framework, it is possible that they could minimize the impact. However, as these changes have happened very recently, it is difficult to predict both the full impact the new framework will have on the challenges noted above and how the new powers and authorities granted to CSIS will interact with the framework.

As the implementation of the revised accountability framework takes place over the coming months and years, it is expected that there will be a certain degree of growing pains as review and oversight entities take up their new roles and the NSI Community adapts to the new requirements. However, the opportunity for self-assessment and review has been built into the new legislation for NSIRA, similar the original legislation that first established CSIS, SIRC and the Inspector General.

Accountability in the CSIS and NSI Community-context is not a one-way process and requires a degree of trust and relationship between CSIS and the entity responsible for conducting review or oversight. CSIS is not, nor cannot be, a complacent participant in the accountability process: it must actively engage with all entities in the accountability framework, from thoroughly apprising the Minister of all necessary information to being open and fulfilling the expected duty of

candour with the judiciary and the Federal Courts. Doing so will improve the effectiveness of the framework and ensure CSIS remains truly accountable.

While this report discusses in-depth the accountability framework for CSIS, there were both limitations and opportunities identified that can be addressed through further research. The focus on CSIS and how the framework functions specifically for this agency prevented delving into the rest of the NSI community and how these departments and agencies intersect on national security matters. It also approached the topic of the NSI accountability framework structure without looking more closely at the informal role external stakeholder expertise has, including expertise from national security policy think thanks and university scholars. Further, it examined accountability from the perspective of the governance structures and did not look more deeply into how challenged related to accountability and oversight are handled by those working in an operational capacity for CSIS. Each of the above identify different areas that deserve further study.

REFERENCES

An Act establishing the Canadian Security Intelligence Service [CSIS Act], Bill C-23, (1985). Retrieved from https://laws-lois.justice.gc.ca/PDF/C-23.pdf

An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism [Anti-terrorism Act, 2001], c. 41 (2001) (enacted). Retrieved from https://laws-lois.justice.gc.ca/PDF/A-11.7.pdf

An Act respecting national security matters [*National Security Act*], Bill C-59, 1st Sess., 42nd Parl., (2019). Retrieved from https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading

Atkinson, M.K. (2019). *Semiannual Report October 2018-March 2019*. Retrieved from the Office of the Inspector General of the Intelligence Community website https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2019/ICIG%20Semiannual%20Report%20-%20October%202018%20to%20March%202019.pdf

Canada: X (Re), 2016 FC 1105. Retrieved from https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/212832/index.do?r=AAAAAQABeAE

Canada: R. v. X (Re), 2017 FC 1048. https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/301967/index.do

Canada: Canada (Attorney General) v. Al Telbani, 2012 FC 474. file:///Users/Olivia/Downloads/D72-94-05%20-%20Tab%205-Canada_(Attorney_General)_v._Al_Telbani,_[20%20-%20A3I1R9.pdf

Canada, Parliament, the Standing Senate Committee on National Finance, Evidence (May 16, 2012). Retrieved from https://sencanada.ca/en/Content/Sen/committee/411/nffn/49566-e

Canada, Parliament, the Standing Committee on Public Safety and National Security, Evidence, Number 089 (December 5, 2017). Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-89/evidence

Canada, Parliament, the Standing Committee on Public Safety and National Security, Evidence, Number 104 (April 17, 2018). Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-104/evidence

Canada, Parliament, the Standing Committee on Public Safety and National Security, Evidence, Number 106 (April 23, 2018). Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-106/evidence

Canada, Parliament, the Standing Senate Committee on National Security and Defence, Number __, (April 10, 2019). Retrieved from https://sencanada.ca/en/Content/Sen/Committee/421/SECD/54681-e

Canadian Civil Liberties Association. (2018). *Civil Society Statement Regarding Bill C-59*. Retrieved from Canadian Civil Liberties Association website https://ccla.org/civil-society-statement-regarding-bill-c-59/

Canadian Civil Liberties Association. (2019). *National Security: National Security Agencies and Accountability.* Retrieved from Canadian Civil Liberties Association website https://ccla.org/focus-areas/national-security/surveillance-and-privacy/

Canadian Security Intelligence Service. (2012). *Public Report 2010-2011.* Retrieved from Government of Canada website https://www.canada.ca/content/dam/csis-scrs/documents/publications/2010-2011PublicReport_English.pdf

Canadian Security Intelligence Service. (2014). *Public Report 2011-2013.* Retrieved from Government of Canada website https://www.canada.ca/content/dam/csis-scrs/documents/publications/PublicReport_ENG_2011_2013.pdf

Canadian Security Intelligence Service. (2017). *Public Report 2014-2016.* Retrieved from Government of Canada website https://www.canada.ca/en/security-intelligence-service/corporate/publications/public-report-2014-2016.html

CBC News. (2014, Feb 21). Whistleblower Edward Snowden's impact on Canada. *CBC/Radio-Canada.* Retrieved from CBC News website https://www.cbc.ca/news/canada/whistleblower-edward-snowden-s-impact-on-canada-1.2546624

Central Intelligence Agency [CIA]. (2016). *Inspector General.* Retrieved from Central Intelligence Agency website https://www.cia.gov/offices-of-cia/inspector-general

Chalk, P. & Rosenau, W. (2004). *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies.* RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/monographs/2004/RAND_MG100.pdf

Chretien, J., Clark, J., Martin, P., Turner, J. et al. (2015, February 19). A close eye on security makes Canadians safer. *Globe & Mail.* Retrieved from http://go.galegroup.com.ezproxy.library.uvic.ca/ps/i.do?p=CPI&u=uvictoria&id=GALE%7CA402196519&v=2.1&it=r&sid=summon

Coats, D.R. (2019). *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community.* Retrieved from Office of Director of National Intelligence website https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Commission of Inquiry into Actions of Canadian Officials in Relation to Maher Arar. (2006). *Report of the Events Relating to Maher Arar: Analysis and Recommendations*. Retrieved from

Government of Canada website http://publications.gc.ca/collections/Collection/CP32-88-1-2006E-AR.pdf

Cronk, E.A. (1985). *Memorandum: the Role of the Inspector General (the "I.G.") and the Security Intelligence Review Committee ("SIRC") Pursuant to the Canadian Security Intelligence Service Act (the "ACT").* Ottawa: ON, Solicitor General of Canada.

Executive Office of the President of the United States [White House]. (n.d.). *President's Intelligence Advisory Board.* Retrieved from the White House website https://www.whitehouse.gov/piab/

Farson, A. S. (1996). In Crisis and in Flux?: Politics, Parliament and Canada's Intelligence Policy. *Journal of Conflict Studies*, 16(1). Retrieved from: https://journals.lib.unb.ca/index.php/JCS/article/view/4524/5346

Farson, A. S. (2000). Parliament and its servants: Their role in scrutinizing Canadian intelligence. *Intelligence and National Security*, 15(2), 225-258. Retrieved from https://doi.org/10.1080/02684520008432609

Forcese, C. & Roach, K. (2015) *False Security: the Radicalization of Canadian Anti-terrorism.* Irwin Law

Forcese, C. & Roach, K. (2016). Bridging the National Security Accountability Gap: A Three-Part System to Modernize Canada's Inadequate Review of National Security. *The Canadian Network for Research on Terrorism, Security, and Society [TSAS]*, 16(4). 1-59. Retrieved from TSAS website http://www.tsas.ca/wp-content/uploads/2018/03/TSASWP16-04_Forcese-Roach.pdf

Forcese, C., Roach, K. & Sherriff, L. (2015). *Bill C-51 Backgrounder #5: Oversight and Review: Turning Accountability Gaps in Canyons?* Retrieved from SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2571245

Gill, P. (1989). Symbolic or real? The impact of the Canadian security intelligence review committee, 1984-88. *Intelligence and National Security,* 4(3), 550-575. Retrieved from https://doi.org/10.1080/02684528908432016

Government of Canada. (1983). *Delicate Balance: A Security Intelligence Service in a Democratic Society: Report of the Special Committee of the Senate on the Canadian Security Intelligence Service*. Ottawa: Government of Canada.

Government of Canada. (2004). *Performance Report for the Department of Public Safety and Emergency Preparedness Canada, 2003-2004*. Retrieved from Government of Canada website https://www.publicsafety.gc.ca/lbrr/archives/cn71026183-2003-04-eng.pdf

Government of Canada. (2013). *2011-2013 Public Report (Canadian Security Intelligence Service).* Retrieved from Government of Canada website

https://www.canada.ca/content/dam/csis-scrs/documents/publications/PublicReport_ENG_2011_2013.pdf

Government of Canada. (2015). *Ministerial Direction to the Canadian Security Intelligence Service: Ministerial Direction for Operations and Accountability.* Retrieved from the Secret Law Gazette: https://secretlaw.omeka.net/items/show/17

Government of Canada. (2016). *Our Security, Our Rights: National Security Green Paper.* Retrieved from Public Safety and Emergency Preparedness Canada website https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf

Government of Canada. (2017a). *National Security Consultations: What We Learned Report.* Retrieved from Public Safety and Emergency Preparedness Canada website https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/2017-nsc-wwlr-en.pdf

Government of Canada. (2017b). *National Security Transparency Commitment.* Retrieved from Government of Canada website: https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html

Government of Canada. (2019). *Commissions of Inquiry.* Retrieved from Privy Council Office website https://www.canada.ca/en/privy-council/services/commissions-inquiry.html

Government of the United Kingdom [Government of the UK]. (2018). *HM Government Transparency Report 2018: Disruptive and Investigatory Powers.* Retrieved from State Watch website http://www.statewatch.org/news/2018/jul/uk-ho-investigatory-disruptive-powers-report-2018.pdf

Government of the United Kingdom [Government of the UK]. (n.d.). *Secretary of State for the Home Department.* Retrieved from the Government of the United Kingdom website https://www.gov.uk/government/ministers/secretary-of-state-for-the-home-department

Government of the United Kingdom [Government of the UK]. (n.d.a). *National Security Council.* Retrieved from the Government of the United Kingdom website https://www.gov.uk/government/groups/national-security-council

Guerin, B., McCrae, J. & Shepheard, M. (2018). *Accountability in modern government: what are the issues?* Retrieved from the Institute for Government website https://www.instituteforgovernment.org.uk/sites/default/files/publications/IfG%20accountability%20discussion%20paper%20april%202018.pdf

Hill, M. (2018). *The Terrorism Acts in 2017.* Retrieved from the Independent Reviewer of Terrorism Legislation website https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2018/10/The_Terrorism_Acts_in_2017.pdf

National Archives of the United Kingdom. (n.d.). *Home Office Appraisal report: 1953-2016.* Retrieved from National Archives of the United Kingdom website http://www.nationalarchives.gov.uk/documents/information-management/home-office-appraisal-report-1953-2016-draft..pdf

Intelligence and Security Committee of Parliament [ISC]. (2013). *Privacy and Security: A modern and transparent legal framework.* Retrieved from Intelligence and Security Committee of Parliament website https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cqG0URhinYo-WVOpIKf2dbqMWLvI8cpALTB9HoHTLwVhScQ-R9BMjVGmFSLsF61B0tlIBzQT64c4isVnFNZyApa11Il457MXehMVaaZYJs9ti4Sc59sZzSLstuZyXO9oBmetEH6vgZI27tt75xGcmWkqa-4g2xK2bWyQqVSNO4NtPIcuSNnrql2ayejMOdGO-HIi6VFUPMWSJk8zlctkL71IKwu-zBdFd-5QO8fia3CM52PD2sA_QG1lYXIJ_1JaaQ8g-Sv&attredirects=0

Investigatory Powers Tribunal [IPT]. (2016). *General Overview and Background.* Retrieved from Investigatory Powers Tribunal website https://www.ipt-uk.com/content.asp?id=10

Inwood, G.J. & Johns, C.M. (2014). *Commissions of Inquiry and Policy Change: A Comparative Analysis.* University of Toronto Press: Toronto Buffalo London. Retrieved from http://web.b.ebscohost.com.ezproxy.library.uvic.ca/ehost/ebookviewer/ebook/bmxlYmtfXzc2MTUzMl9fQU41?sid=c9c7f4d9-f4df-4acf-bddc-26d4cecc6258@pdc-v-sessmgr05&vid=1&format=EB&rid=1

Kim, S. & Perlin, P. (2019, March 25). *Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance.* Lawfare blog. Retrieved from: https://www.lawfareblog.com/newly-disclosed-nsa-documents-shed-further-light-five-eyes-alliance

Lagasse, P. (2010). Accountability for National Defence: Ministerial Responsibility, Military Command and Parliamentary Oversight. *IRPP Study*, 4, 1-64. Retrieved from: https://www-deslibris-ca.ezproxy.library.uvic.ca/ID/222101

Larsen, M. & Walby, K. (2012). *Brokering Access: Power, Politics, and Freedom of Information in Canada.* Retrieved from https://books.google.ca/books?hl=en&lr=&id=lT70A82o9DgC&oi=fnd&pg=PR7&dq=%22accountability+framework%22+%22national+security%22+canada&ots=rORYFCFg4E&sig=dpKGBu4khx8fQpXFHpk4TkEDTas#v=onepage&q=%22accountability%20framework%22%20%22national%20security%22%20canada&f=false

Littlewood, J. (2011, October 28). Intelligence, accountability and privacy versus globalization: is Parliament up to the task? *The Hill Times.* Retrieved from https://www-hilltimes-com.ezproxy.library.uvic.ca/2011/10/28/intelligence-accountability-and-privacy-versus-globalization-is-parliament-up-to-the-task/18654

MacCharles, T. (2017, June 23). Public Safety Minister Ralph Goodale says national security agencies welcome more oversight. *Toronto Star (Online)*. Retrieved from ProQuest website: https://search-proquest-com.ezproxy.library.uvic.ca/docview/1912933549?pq-origsite=summon

MacAskill, E. & Hern, A. (2018, June 4). Edward Snowden: "The people are still powerless, but now they're aware". *The Guardian.* Retrieved from the Guardian website: https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware

McDonald, D.C. (1981). *Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police – Second Report: Freedom and Security Under the Law*. Ottawa, Ontario: Privy Council Office.

Mitrovica, A. (2015, April 10). Ex-spy watchdog Plunkett calls CSIS civilian review 'a joke'. *iPolitics.* Retrieved from https://ipolitics.ca/2015/04/10/ex-spy-watchdog-plunkett-calls-csis-civilian-review-a-joke/

National Archives. (n.d.). *Newly released GCHQ files: UKUSA Agreement.* Retrieved from National Archives website: https://www.nationalarchives.gov.uk/ukusa/

Office of the Auditor General of Canada. (2003). *Report of the Auditor General of Canada to the House of Commons: Chapter 10: Other Audit Observations.* Retrieved from Government of Canada website http://www.oag-bvg.gc.ca/internet/docs/20031110ce.pdf

Office of the Auditor General of Canada. (2004). *Report of the Auditor General of Canada to the house of Commons: Chapter 3: National Security in Canada – The 2001 Anti-Terrorism Initiative.* Retrieved from http://www.oag-bvg.gc.ca/internet/English/parl_oag_200403_03_e_14895.html

Office of the Prime Minister. (2015). *Open and Accountable Government.* Retrieved from the Office of the Prime Minister of Canada website https://pm.gc.ca/en/news/backgrounders/2015/11/27/open-and-accountable-government

Office of the Director of National Intelligence [ODNI]. (2017). *ODNI Factsheet.* Retrieved from Office of the Director of National Intelligence website https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf

Investigatory Powers Commissioner's Office [IPCO]. (2018). *What we do.* Retrieved from Investigatory Powers Commissioner's Office website https://www.ipco.org.uk/

Parliament of Canada. (2019). *Responsible Government and Ministerial Accountability.* Retrieved from https://www.ourcommons.ca/About/Compendium/ParliamentaryFramework/c_d_responsiblegovernmentministerialaccountability-e.htm

Parliament of the United Kingdom [UK]. (n.d.). *Ministerial responsibility.* Retrieved from Parliament of the United Kingdom website https://beta.parliament.uk/articles/CuEfCuHX

Privy Council Office. (2001). *The Canadian Security and Intelligence Community: Helping Keep Canada and Canadians Safe and Secure.* Retrieved from Government of Canada website http://publications.gc.ca/collections/Collection/CP32-74-2001E.pdf

Public Safety Canada. (2016). *2016 Public Report on the Terrorist Threat to Canada.* Retrieved from Government of Canada website https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-pblc-rpr-trrrst-thrt/2016-pblc-rpr-trrrst-thrt-en.pdf

Public Safety Canada. (2019). *2018 Public Report on the Terrorist Threat to Canada (3rd revision).* Retrieved from Government of Canada website https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrsm-thrt-cnd-2018/pblc-rprt-trrrsm-thrt-cnd-2018-en.pdf

Rankin, M. (1986). National Security: Information, Accountability, and the Canadian Security Intelligence Service. *The University of Toronto Law Journal*, 36(3), 249-285. Retrieved from https://www.jstor.org/stable/825575

Rempel, R. (2004). Canada's Parliamentary Oversight of Security and Intelligence. *International Journal of Intelligence and CounterIntelligence,* 17(4), 634-654. Retried from https://doi.org/10.1080/08850600490496443

Rockefeller, N.A. (1975). *Report to the President by the Commission on CIA Activities within the United States.* Retrieved from the Mary Ferrell Foundation website https://www.maryferrell.org/showDoc.html?docId=930#relPageId=1&tab=page

Rosen, P. (2000). *The Canadian Security Intelligence Service.* Retrived from the Government of Canada website: http://publications.gc.ca/collections/Collection-R/LoPBdP/CIR/8427-e.htm

Ryan, J.F. (1989). The Inspector General of the Canadian Security Intelligence Service. *The Journal of Conflict Studies,* 9(2), 33-51. Retrieved from https://journals.lib.unb.ca/index.php/JCS/article/view/14844

Security Intelligence Review Committee. (1985). *Annual Report 1984-85.* Retrieved from Government of Canada website http://www.sirc-csars.gc.ca/pdfs/ar_1984-1985-eng.pdf

Security Intelligence Review Committee. (1986). *Annual Report 1985-86.* Retrieved from http://www.sirc-csars.gc.ca/pdfs/ar_1985-1986-eng.pdf

Security Intelligence Review Committee. (1988). *Annual Report 1987-88.* Retrieved from Government of Canada website http://www.sirc-csars.gc.ca/pdfs/ar_1987-1988-eng.pdf

Security Intelligence Review Committee. (1990). *Annual Report 1989-90.* Retrieved from Government of Canada website http://www.sirc-csars.gc.ca/pdfs/ar_1989-1990-eng.pdf

Security Intelligence Review Committee. (1995). *Annual Report 1994-95.* Retrieved from Government of Canada website http://www.sirc-csars.gc.ca/pdfs/ar_1994-1995-eng.pdf

Security Intelligence Review Committee. (2001). *Annual Report 2000-2001.* Retrieved from Government of Canada website http://www.sirc-csars.gc.ca/pdfs/ar_2000-2001-eng.pdf

Security Intelligence Review Committee. (2002). *Annual Report 2001-2002.* Retrieved from Government of Canada website http://www.sirc-csars.gc.ca/pdfs/ar_2001-2002-eng.pdf

Security Intelligence Review Committee. (2014). *Annual Report 2013-2014.* Retrieved from Government of Canada website http://www.sirc-csars.gc.ca/pdfs/ar_2013-2014-eng.pdf

Security Service. (n.d.). *Law and Governance.* Retrieved from Government of the United Kingdom [UK] website www.mi5.gov.uk/zh-hans/law-and-governance

Security Service. (n.d.a.). *Threat Levels.* Retrieved from Government of the United Kingdom [UK] website https://www.mi5.gov.uk/threat-levels

Wark, W. (2015). *Once More into the Breach.* Retrieved from the Canada2020 website http://canada2020.ca/wp-content/uploads/2015/03/Canada-2020-Research-Once-More-Into-the-Breach-Wark-2015.pdf

Weller, G.R. (1988). Accountability in Canadian intelligence services. *International Journal of Intelligence and Counter Intelligence,* 2(3). DOI: 10.1080/08850608808435074

Whitaker, R. (1992). The politics of security intelligence policy-making in Canada: II 1984-91. *Intelligence and National Security,* 7(2), 53-76. Retrieved from https://doi.org/10.1080/02684529208432156

Whitaker, R. (1996). The 'Bristow affair': A crisis of accountability in Canadian security intelligence. *Intelligence and National Security,* 11(2), 279-305. Retrieved from https://doi.org/10.1080/02684529608432357

White House. (n.d.). *President's Intelligence Advisory Board.* Retrieved from the Executive Office of the President of the United States website https://www.whitehouse.gov/piab/

APPENDIX

List of Questions for Interviews

1. What organizations within the National Security and Intelligence (NSI) Community have you worked for (including regular, contractual, or consulting employment)?

    a. How long were you in each position?

2. What was your role within the NSI organization?

    a. What activities did you take part in (e.g. policy development, communications)?
    b. Have you worked in roles where conducting activities related to Ministerial oversight and NSI accountability was one of your primary functions?
    c. Which department or agency did you act in this role with?
    d. Please give an example (if possible) of a specific policy or project you worked on in these positions (specifically related to Ministerial oversight/accountability of a governmental department or agency).

3. Why did you accept a position in the department or agency, or previous organizations, with an accountability or Ministerial oversight function?

4. Were you employed by your organization during a transition period for the NS accountability framework or Ministerial oversight? (e.g. the elimination of the Inspector General in 2012)

    a. If yes, what were the impacts of the changes on your role within the organization?
    b. If yes, what were the overall impacts of the changes on the role of the organization in the accountability framework?
    c. Did these impacts have a positive effect, or negative, to NSI accountability and Ministerial Oversight?

5. What role does/did Ministerial oversight or NSI accountability have on your day-to-day activities as an employee of your organization(s)?

6. What is your understanding of the role of accountability and Ministerial Oversight for CSIS?

7. What challenges do you see that might arise from the implementation of Bill C-59? (the creation of NSIRA, Intelligence Commissioner)

8. Are there other areas of NSI accountability and Ministerial oversight of CSIS that could be addressed in future legislation or organizational changes?

List of Figures

Figure 1: 1984 Accountability Framework for CSIS

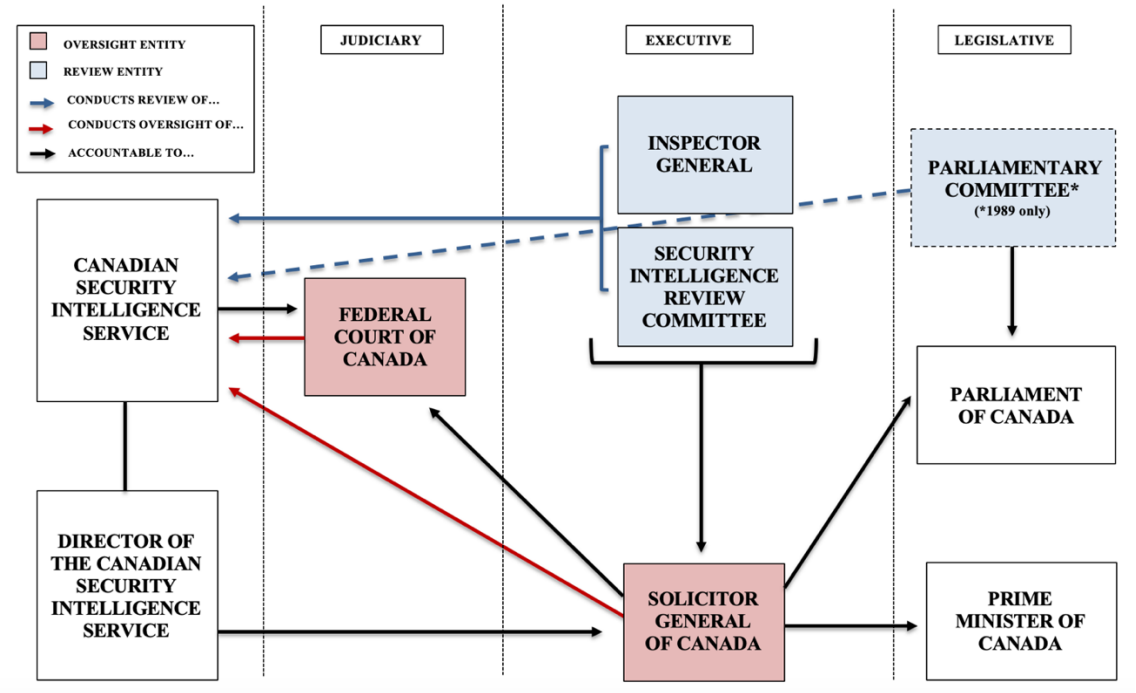


Figure 2: 1984 Analytical Framework for CSIS Accountability

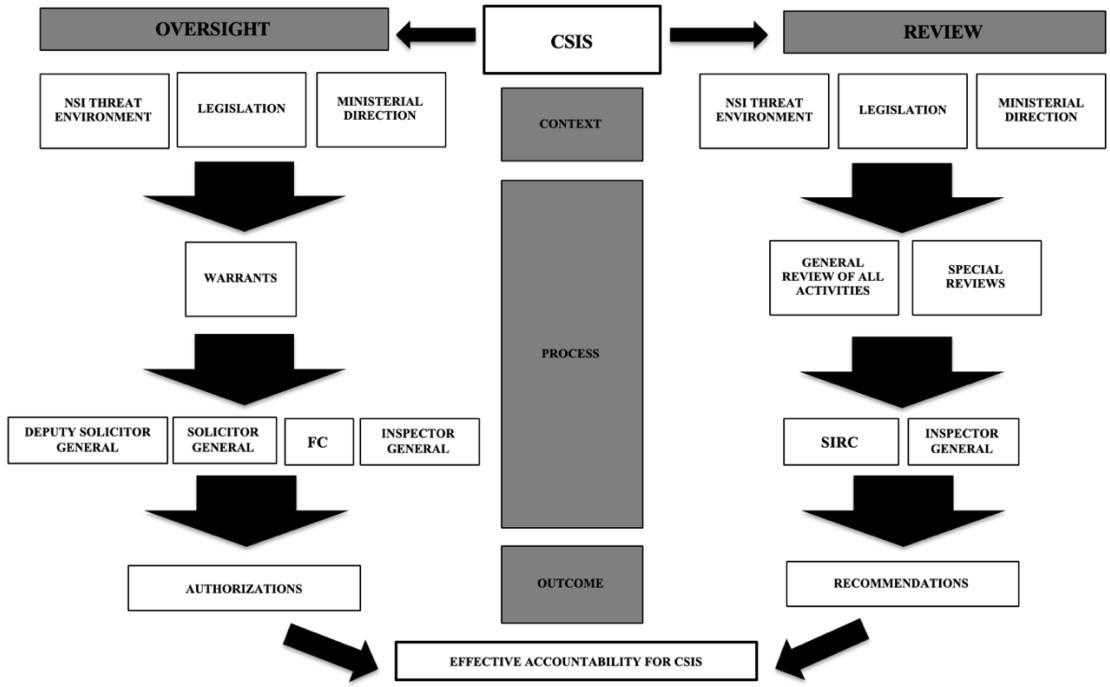


Figure 3: 2012 Accountability Framework for CSIS

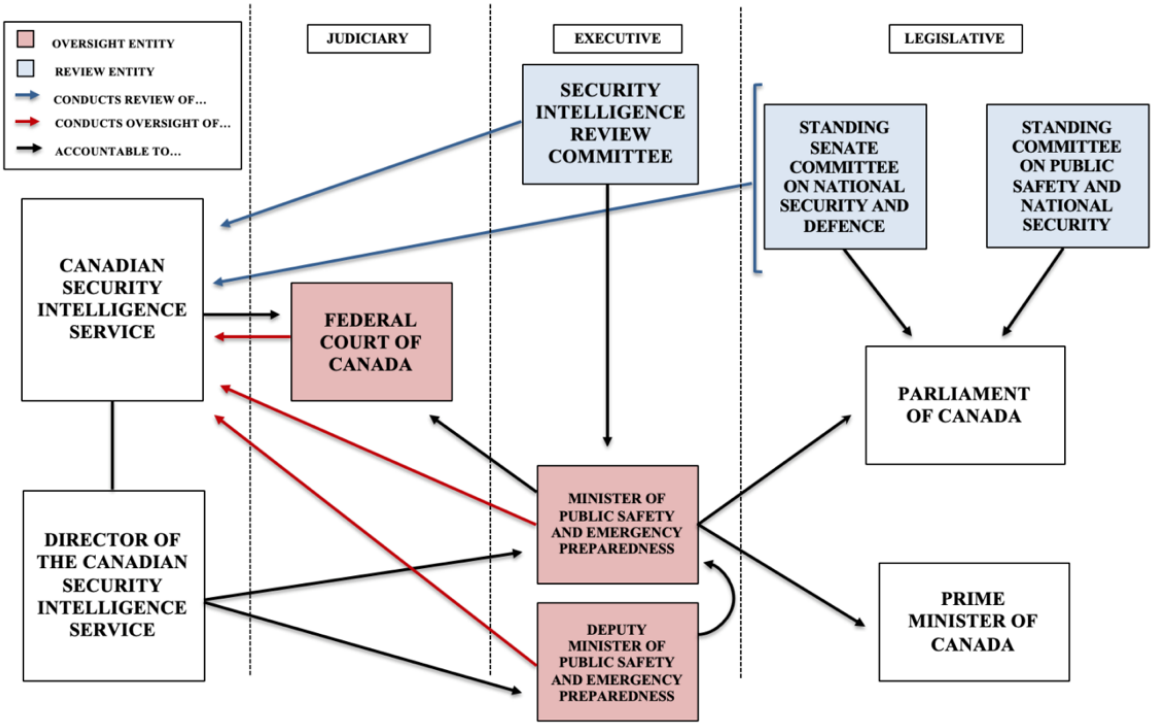


Figure 4: 2019 Accountability Framework for CSIS

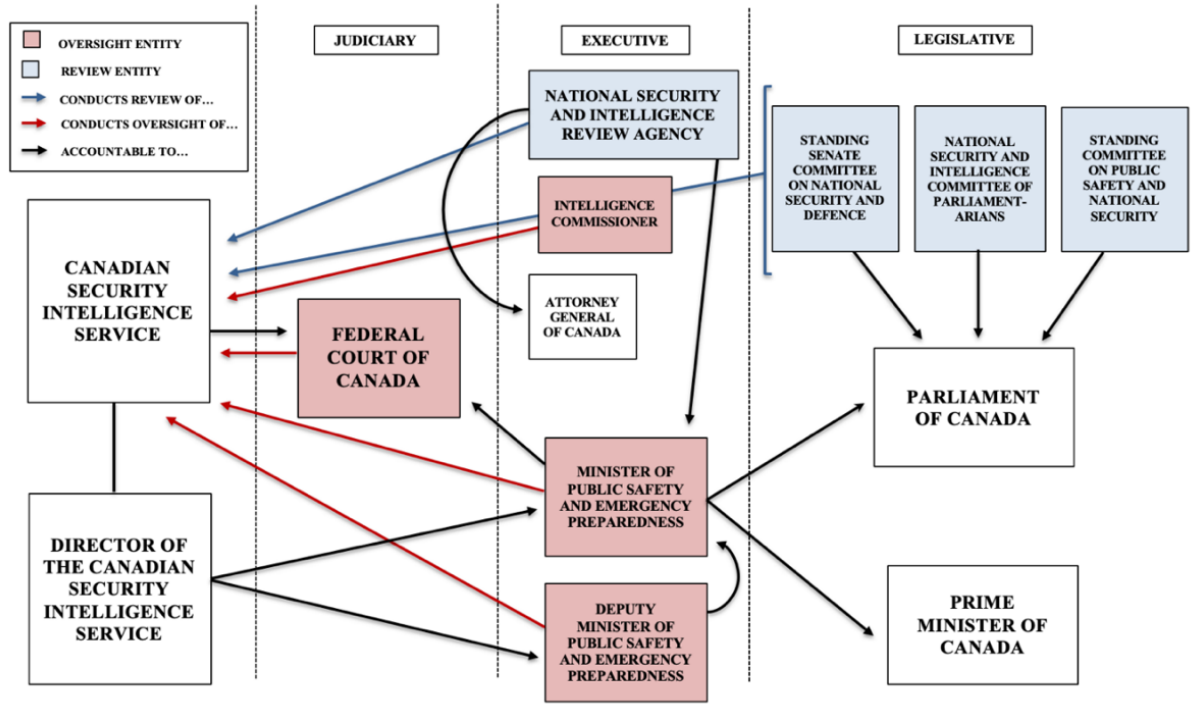
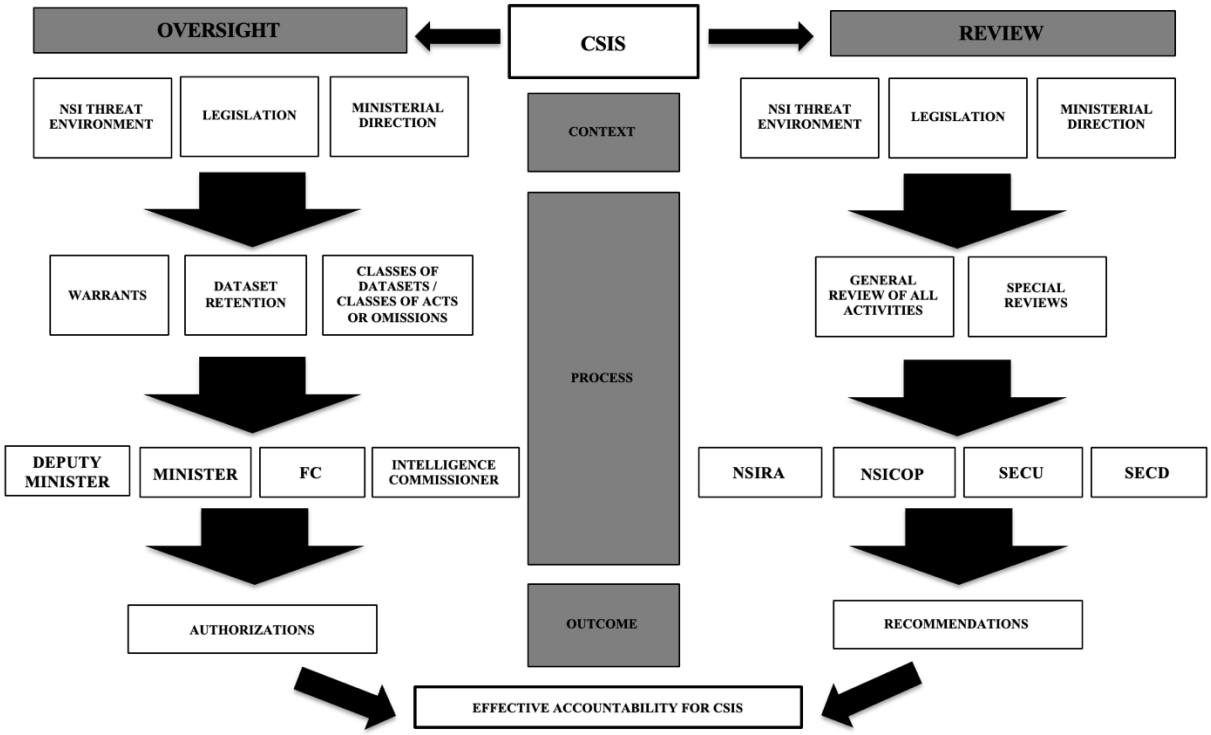


Figure 5: 2019 Analytical Framework for CSIS Accountability



List of Tables