Bill C-51 Backgrounder #5:

Oversight and Review: Turning Accountability Gaps into Canyons?

Craig Forcese[*] and Kent Roach[**]
with Leah Sherriff[***]

Executive Summary

Given the length of this backgrounder, we include this executive summary.

Canada's system of national security oversight is imperfect. Its system of national security review, meanwhile, is frayed, and perhaps even close to broken. Bill C-51 will accelerate this pattern. Without a serious course correction, we risk serious accountability challenges in national security law, and the prospect of often avertible security service scandals.

"Review" and "oversight" are often confused. Oversight is a real-time (or close to real time) operational command and control strategy. Review is a retrospective performance audit, examining past security service activity and gauging it against specific criteria (e.g., compliance with law and policy).

Oversight in Canada is usually an executive branch function, and in some cases is supposed to be exercised at the ministerial level. This system has not always worked well. For instance, the Air India Commission raised concerns that ministerial oversight was not sufficient and proposed that the Prime Minister's National Security Advisor play an oversight role in resolving disputes between CSIS and the RCMP. The government rejected this recommendation for enhanced oversight but then in bills C-44 and C-51 proposes giving CSIS new privileges and powers that make enhanced oversight in the public interest even more important.

Judges in Canada also may play an oversight role of sorts. For instance, in defending bill C-51, the government places much reliance on judicial warrants authorizing the new CSIS powers. Critically, this argument overstates the virtues of the Federal Court warrant system. First, CSIS will *not* require warrants for every exercise of its new powers. The only circumstance in which the bill clearly requires a warrant is when CSIS "will" (not "may") contravene a Charter right or be contrary to other Canadian law. As with its existing surveillance powers, a substantial amount of CSIS activity that falls short of the warrant "trigger" will *never* be pre-authorized by a judge. This is especially true in international operations: places where Canadian law and the Charter generally do not apply and thus are not contravened.

---

[*] Associate Professor of Law, University of Ottawa

[**] Professor of Law, University of Toronto

[***] JD Candidate, University of Toronto

Second, warrants will (and always have been) issued in a secret, private proceeding in which only the government side is represented. There, judges are especially dependent on full candour by the government, a standard that has not always been achieved. But even with full candour, government positions will be just that: government positions. In the absence of persons with the means, incentive and (most importantly) full access to the facts necessary to challenge government positions, such legal proceedings are inherently one-sided. It is important to acknowledge that even in the presence of the most exacting judge, and even with the fullest candour by the government, mistakes will be made. This is and always will be a problem with warrants. Mistakes when authorizing CSIS actions that go beyond surveillance and include physical actions (short of bill's outer limit of intentional or negligent bodily harm, invasion of sexual integrity or obstruction of justice) are more grave than threats from undue surveillance.

At core, the system of judicial oversight adopted by bill C-51 accepts risks of mistakes. For instance, bill C-51 does not incorporate the existing system of special advocates into its processes. As imperfect as that approach may be, it would be better than the only alternatives: judges sitting alone in the presence only of the government or supported by an *amicus curiae* (friend of the court) whose role may be quite attenuated.

More than this, even where a warrant is required, Federal Court judges are in a poor position to evaluate what is then done under their authority. There is no formal "feedback" loop requiring CSIS to report back and account for its conduct. To the extent we can know these things, in the past, where Federal Court judges learned of a failure to comply with the full letter of a warrant, this has been largely a fortuitous accident.

In the result, Federal Court judges will be left on their own to devise accountability structures to ensure that CSIS does not go beyond what is authorized in the warrant. They may insist, for example, on "reporting back" requirements, or may impose an obligation in the warrant that the minister request a "special report" from SIRC on the subsequent execution of the warrant. We believe that these sorts of conditions will be vital in correcting "accountability gaps" in the present system, but we also recognize that they will place strains on the small budget ($3 million annually) and staff (17 plus executive director) of SIRC.

Whether courts choose to pursue this path is not a matter that the public will be able to evaluate, since CSIS warrants are secret and not made public. In consequence, accountability may depend on vigorous and thorough review by CSIS's review body, SIRC, acting under its regular authority.

One should not assume that such vigorous and through review will be possible.

For one thing, judges may issue "assistance orders" under the new powers, ordering "any person" to provide assistance to CSIS in the execution of a warrant power, and CSIS can enlist participation by other parties. These other persons could include federal officials who are not subject to *any* independent review.

Even where there are review structures, it would be a serious error to assume that review reaches all security service conduct. Review is a partial audit – a sampling of agency conduct. SIRC has never had the capacity to examine CSIS's total range of conduct, or indeed even all of CSIS's range of conduct under its *existing* warrants. A sampling approach to review will become even more partial as CSIS's powers expand, while SIRC remains underresourced and staffed.

More than this, both the Arar Commission and SIRC's own public statements and documents underscore that SIRC's legal powers are too narrowly drawn, especially given CSIS's increased interaction with other departments and agencies. While bill C-51 contemplates a "whole-of-government" approach to security, Canada's review bodies remain "stovepiped" by agency. Since, as former SIRC chair Chuck Stahl observed, the review "trail is not going to stop nicely and neatly at CSIS's door,"[1] a substantial amount of Canadian government national security activity is immunized from independent review.

In direct consequence, the Arar Commission recommended that SIRC's jurisdiction be expanded to include other agencies and that "statutory gateways" be created that would allow it to share secret information and conduct joint investigations with the CSE Commissioner and the RCMP review body, Canada's two other existing independent national security review bodies.

That was a reasonable proposal 10 years ago, and would mark an enormous improvement over the status quo. But it no longer suffices.

The pace of change in the national security sector, coupled with the expansion of security service powers in bill C-51 (and bill C-44), counsel an equivalent large-scale renovation of the accountability side. There is a compelling need for a better resourced expert review body with a remit that encompasses all of the government's national security activities. A "super-SIRC" with whole of government jurisdiction would amount to a "catch-up" on what the Australians have done (for some time) with that country's Inspector General of Intelligence and Security and mirror evolving practices in other democracies.

And finally, there is also a critical need for "pinnacle" review. Even a super-SIRC will review a subset of national security activities. It would focus on more than its one, current "tree", but would still not be able to see the full national security "forest". In our system, no independent body sees the "forest". This is exactly the review function performed in most other Western democracies by a specialized parliamentary review committee.

A parliamentary committee is not a redundancy – it is a supplement to expert committee review. A parliamentary committee will review performance after the fact and not exercise command and control oversight. We underscore again: this role as

---

[1] The SIRC Chair Chuck Strahl to the Senate's Standing Committee on National Security and Defence,*Minutes of Proceedings and Evidence*, 41st Parl, 2nd Sess, (9 December 2013), available online: http://www.parl.gc.ca/content/sen/committee/412%5CSECD/51109-E.HTM

"pinnacle" reviewer is accomplished no where else in our system and is concerned with both the propriety and efficacy of our national security systems.

Past experience in other democracies (and especially Australia) suggests that expert and parliamentary review may work effectively together. They can also contribute to desperately required Parliamentary and public competence in national security law.

About this project

This is a working document. It is legal scholarship done in "real time" in a highly politicized environment, in which fundamental decisions about the shape of law are being made.

There will be typos and glitches! We shall continue to develop this paper and its counterparts on different aspects of nill C-51, adding more discussion, references and footnoted sources. We also anticipate developing the ideas and conclusions we present.

Accordingly, we welcome (and very much encourage and need) feedback, critiques, suggestions and observations from other lawyers, legal scholars, security experts and other interested persons with expertise to contribute (whether practical, legal, scholarly). We are, in other words, calling for a "crowdsourced" response to bill C-51, and in this paper, to the question of oversight and review.

We add an additional word relevant to this, a document dealing with CSIS. We are legal academics who have been researching and writing on issues of national security law (Canadian, international and comparative) for a sum total of 26 person years (between the two of us). We have never worked in a security service. Instead, one or both of has worked with (or been involved in) two commissions of inquiry examining the security services (the Arar and Air India inquiries), a number of national security cases in the courts and several other commissions of inquiry focusing on state wrongdoing, including in the criminal justice sector. We are, in other words, an occasional and minor part of the national security "accountability sector", to the extent that such a thing exists in Canada.

Our legal expertise informs our legal conclusions. Our accountability perspective and experience informs our comments on operational issues.

There will be those who disagree with us, especially in relation to our specific reform proposals. We invite debate and discussion. That is the very reason we are conducting this project. These issues are too important to be swept up in partisan political positioning and infighting, and the debate should be informed and acute.

Please send feedback to: cforcese@uottawa.ca and kent.roach@utoronto.ca

Table of Contents

Introduction 7
Part I: Oversight versus Review 8
A. Oversight of National Security 9
1. Effective Executive Oversight 13
a) Concerns 13
b) Comparative Oversight 15
2. Limits of Judicial Oversight 16
a) No Serious Prospect of Judicial Scrutiny of Information Sharing 16
b) Judicial Warrants only Required for Some CSIS Powers 16
iii) Judicial Warrants and Procedural Shortcomings 17
3. Parliamentary Role in Oversight 21
B. The Concept of Review 23
1. Basic Principles 23
2. Elements of Effective Review 24
Part II: Review in Canada 25
A. Overview 25
B. SIRC in Context 27
1. Past Academic Assessments 27
b. Contemporary SIRC Review 29
1. Staffing 29
2. Budget 29
3. Access to Secret Information 31
5. Review Functions and Challenges 32
C. Need for Enhanced Review 37
1. Reform Options 40
a) Getting Rid of Silos 40
ii) Expanded Review as Proposed by the Arar Commission 41
iii) 'Super SIRC': Whole of Government National Security Review 42
2. Comparative Developments in Review Reform 43
B. Parliamentary Review 45
1. Conventional Role of Parliamentary Committees 45
2. National Security Committee of Parliamentarians 46
3. More Recent Developments 49
4. Concerns about Overreach and Redundancy 50
Conclusion 52

Introduction

Under bill C-51, CSIS's powers will expand significantly. The proposed changes are the most dramatic since the Service was created in 1984. We describe these changes in detail in backgrounder #2, posted to www.antiterrorlaw.ca. Bill C-51 responds by superimposing limited judicial oversight. A warrant will not, however, be required in every instance where CSIS exercises its new powers. Where they are required, warrants will be granted in one-sided or ex parte hearings and will be unlikely to be appealed. Moreover, there is no mechanism to audit CSIS's performance under warrants. It will left to individual Federal Court judges to devise what, if any, "reporting back" is done to ensure that CSIS and perhaps other partner agencies do not go farther than is authorized by the warrant.

The existing CSIS review body – the Security Intelligence Review Committee – is tasked with reviewing some "aspect" of the new power. It is not instructed to assess its every use. Indeed, "review" in the Canadian context has always depended on partial audits, and not full assessments. These partial audits risk becoming more partial as CSIS's operations and scale increase, while SIRC's powers and resources remain unchanged, even as it must assume additional responsibilities.

Although all democracies are struggling with accountability gaps as they engage in intensified and integrated "whole of government" approaches to security, Canada suffers from a particularly wide "accountability gap".

Only three of agencies are subject to any sort of national security review (CSIS, RCMP and CSE), and they are review be three separate review bodies (SIRC, RCMP (Civilian Review and Complaints Commission, and the CSE Commissioner). As the Arar Commission found in 2006, this means that the review agencies remain "siloed" or "stovepiped", even while the agencies are (quite appropriately) working together.

In addition, many other agencies and departments with national security responsibilities, including the other 14 agencies designated as recipient institutions for information sharing are subject to no independent national security review. They are reviewed by the Privacy Commissioner but only for privacy concerns and with powers that the Privacy Commissioner pronounced inadequate in a 2014 report.[2]

Almost 10 years ago, the Arar commission of inquiry concluded that this mismatch between state power and accountability was unsustainable, and proposed both broadening the number of agencies subject to review and facilitating cooperation between existing review bodies, something stymied by law and government practice at present. The present government has declined to implement these recommendations, and fails again to address them in bill C-51, the single greatest expansion of national security powers since 9/11.

---

[2] Office of the Privacy Commissioner Special Report to Parliament on Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance, January 28, 2014 at https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp

In the result, considerable discussion must now focus on the question of "accountability". Since bill C-51 has been tabled, much of that discussion has invoked "oversight", although it is apparent that not everyone means the same thing in using that term.

This document serves as a primer on the question of accountability and national security. We focus on two sorts of accountability: oversight and review. We begin by distinguishing between these two discrete concepts. We then focus on how oversight operates in Canada, examining its limits. Then we turn to review, examining in detail criteria for effective review and then assessing the CSIS review body, SIRC. We also discuss Parliament and the concept of parliamentary review.

Part I: Oversight versus Review

We begin by underscoring the important distinction in Canadian national security law between "oversight" or "review". These terms are often misunderstood, and even knowledgeable commentators invoke "oversight" when discussing accountability of every sort. Loose language is a real danger and without conceptual clarity about the different nature and ambitions of review and oversight, there may be disappointment and confusion even if reforms are implemented.

Put simply, in Canadian practice, "oversight" is command/control over operations (what one might call *real time* or close to real time governance). In relation to CSIS, for example, executive chains of command (up to and including the minister of public safety) perform "oversight", as does (in essence) the Federal Court in the form of search and surveillance warrants.

"Review" is after-the-fact auditing of operations, measured against some set of criteria (e.g., compliance with the law or policy) (what one might call *ex post facto* accountability). A reviewer does not have operational responsibility for what is being reviewed and this helps ensure that reviewers remain independent and are not complicit, or seen to be complicit, in what is being reviewed.

Moreover, while robust oversight involves judicial and/or executive authorization for *each* individual activity (or classes of activity), review is a *partial* assessment. Review depends on a "sampling" of past conduct or an audit. Not every activity or even class of activities is audited, and certainly not audited annually or in anything close to real time. This fundamental structural distinction must be kept in mind in assessing review as an effective form of accountability.

In Canada, what most people mean when they invoke "oversight" in popular discussion is actually "review". In relation to CSIS, the Security Intelligence Review Committee (SIRC) performs review. Review bodies, including SIRC, make findings and recommendations about past CSIS conduct. They report on this conduct, but do not have the power to require CSIS to change its behaviour.

In Canada, there is no parliamentary "oversight" in national security – oversight in the sense defined here is not something done by true legislative bodies in any

jurisdiction we have studied. "Review" is, however, a common enterprise for bodies comprising legislators. Indeed, a 2011 comparative study by the European Parliament, suggests Canada is close to unique now among Western democracies in having no serious parliamentary review (or at least review in which parliamentarians participate).[3] That comparative experience underscores that effective and credible review of national security activities requires unfettered access to secret information, even if there are restrictions on subsequent publication that may reveal secrets. Again, Canada measures poorly against this standard. Canada, alone among its "5 eyes" partners (US, UK, Australia and New Zealand) does not give any parliamentarian access to information that is classified as secret. As such, there is no parliamentary "review" in Canada. We discuss parliamentary functions below.

A. Oversight of National Security

It is not possible in this backgrounder to explore the full range of oversight mechanisms in Canadian national security law. In Table 1 we set out some of the tools, applicable to CSIS, the RCMP and Canada's signals intelligence agency, CSE.

Table 1: Examples of National Security Oversight in Canadian Law

Agency	Executive Oversight	Judicial Oversight
CSIS	CSIS is headed by a director, charged with the "control and management of the Service" under the direction of the minister of public safety.[4] The latter is specifically empowered to "issue to the Director written directions with respect to the Service."[5] The director, meanwhile, is obliged to consult the deputy minister of public safety on "the general operational policies of the Service" and on any other matter that the minister directs.[6] These and other provisions in the Act create a more aggressive level	In its present form, the CSIS Act creates a judicial warrant system for intelligence collection. CSIS may apply for such a warrant if it "believes, on reasonable grounds, that a warrant ... is required to enable the Service to investigate a threat to the security of Canada" or to assist the minister of national defence in "the collection of information or intelligence relating to the capabilities, intentions or activities of ... any foreign state or group of foreign states."[8] This CSIS warrant provision is a mild variation on conventional surveillance warrants, and has withstood constitutional challenges for that reason.[9] The *only* constitutional right at issue with security intelligence warrants is the protection against unreasonable search and seizure. In the world of search and seizure, judicial warrants are designed to prevent - not authorize - Charter violations. That is

[3] Aiden Wills, Ashley Thornton, Hans Born, Martin Scheinin, Mathias Vermeulen, Micha Wiebusch, *Parliamentary Oversight of Security and Intelligence Agencies in The European Union* (Brussels: European Parliament, 2011), available at http://issat.dcaf.ch/content/download/4148/36754/file/Parliamentary%20Oversight%20of%20Security%20and%20Intelligence%20Agencies%20in%20the%20European%20Union.pdf.

[4] CSIS Act, subs. 6(1).

[5] CSIS Act, subs. 6(2).

[6] CSIS Act, s. 7.

Agency	Executive Oversight	Judicial Oversight
	of political oversight than exists for the RCMP, discussed below. Indeed, oversight extends into CSIS investigations. A CSIS warrant application can only be made (or renewed) before a Federal Court with ministerial authorization.[7]	because the Charter privacy protection is qualified – s.8 of Charter protects against "unreasonable" searches and seizures and a search under a warrant is prima facie proper. Moreover, if CSIS did not have a warrant, it would violate the Criminal Code Part VI prohibitions on unauthorized wiretaps. The "trigger" – the circumstance in which CSIS must obtain a warrant – is when its conduct transgresses the reasonable expectation of privacy guarded by s.8 of the Charter.[10] Short of this "trigger", CSIS need not seek or obtain a warrant. Under the system proposed in Bill C-51, CSIS would be empowered to take "measures" inside or outside Canada to "reduce the threat" to the security of Canada. The government calls this "disruption", which we believe is an underinclusive expression. Therefore, for ease of reference, we call this a "kinetic" power to do things to people or things in the real world. Where these measures involve conduct that would break Canadian law or contravene a Charter right, it must seek a Federal Court warrant. In backgrounder #2, we examine at length the extent to which this system is a significant rupture with the past, is not at all analogous to regular search warrants and seems to violate very fundamental doctrines of Canadian constitutional law. Note that nothing in C-51 obliges CSIS to seek a warrant unless there measure will contravene Canadian law or the Charter. Put another way, warrants will not be required in every instance where

8 CSIS Act, R.S.C. 1985, c. C-23, s. 21, cross-referenced to s. 16.

9 See *Atwal*, [1988] 1 F.C. 107 at para. 36. Also, in *Canadian Civil Liberties Assn. v. Canada (Attorney General)*, (1998) 40 O.R. (3d) 489 (Ont. C.A.), the Canadian Civil Liberties Association sought to challenge the CSIS Act provisions on s. 8 grounds. The Ontario Court of Appeal refused them public interest standing to do so, concluding, *inter alia*, that the arguments presented by the CCLA on the s. 8 violation were "weak." *Ibid*. at para. 88.

7 CSIS Act, ss. 21 & 22.

10 *Mahjoub (Re)*, [2013] F.C.J. No. 1217 at para. 33 ("Parliament intended these [warrant] provisions to be used in circumstances where the investigation required interference with an individual's reasonable expectation of privacy. In such cases, the Service is required to obtain judicial authorization.")

Agency	Executive Oversight	Judicial Oversight
		CSIS might act.
RCMP	The RCMP is headed by a commissioner who, "under the direction of the Minister [of public safety], has the control and management of the Force."[11] In reality, however, the level of ministerial direction is constrained by the concept of police independence. Police independence is a common law construct,[12] now with a constitutional imprimatur.[13] At core, it means that the police (in performing at least their criminal investigation role) are not agents of the Crown or under the direction of the political executive. This doctrine attempts to remove political influence from ordinary police decision-making. Police independence is acceptable in criminal investigations for one reason: that task is a reasonably transparent one, amenable to scrutiny in the courts either as a collateral issue in a criminal trial once charges are laid or in abuse of process or power proceedings. National security investigations – even if nominally directed at bringing criminal charges in order to comply with the RCMP's core	Unlike CSIS operations, police investigations are mostly about law enforcement and ideally culminate in prosecutions in open courts. In this respect, court proceedings act as a form of "back end" accountability for police that does not exist for CSIS, except in rare instances where something goes amiss in a CSIS investigation and that is revealed as part of a subsequent court case. Courts also perform an "oversight" role during investigations, authorizing, e.g., electronic surveillance under Part VI of the Criminal Code or otherwise issuing search (or arrest) warrants.

[11] RCMP Act, s. 5.

[12] See, most famously, *Ex Parte Blackburn*, [1968] 1 All E.R. 763 at 769 (Eng. C.A.) ("every constable in the land ... should be, and is, independent of the executive. ... [H]e is not the servant of anyone, save of the law itself. No Minister of the Crown can tell him that he must, or must not, keep observation on this place or that; or that he must, or must not, prosecute this man or that one. Nor can any police authority tell him so. The responsibility for law enforcement lies on him. He is answerable to the law and to the law alone").

[13] *R v. Campbell*, [1999] 1 S.C.R. 565 at para. 29 (in criminal investigations, "police are independent of the control of the executive government" and noting that this principle "underpins the rule of law," a constitutional concept).

Agency	Executive Oversight	Judicial Oversight
	policing mandate – are conducted more clandestinely and do not always or even often lead to prosecutions before courts.[14] For this reason, full-blooded police independence in the national security context might convert independence into a species of impunity, producing a police force unaccountable to anyone. In 2006, the Arar commission effectively endorsed the present level of oversight, while recommending a substantial redesign in the *ex post* review of RCMP national security activities. Review of national security functions is discussed separately below.	
CSE	CSE is a "signals" (or electronic) intelligence agency. Among other things, CSE collects "foreign intelligence". CSE's law recognizes that "there may be circumstances in which incidental interception of private communications or information about Canadians will occur."[15] The law permits the Minister of National Defence (currently Jason Kenney) to issue a "ministerial authorization" authorizing CSE to collect "private communications". The minister may issue this authorization only where satisfied, among other things, that the interception is directed at foreign entities outside of Canada	There is no direct judicial oversight of CSE. One of us has argued that this deficiency, applied to CSE's activities that may involve intercepts of Canadian data in which there is a reasonable expectation of privacy, is unconstitutional and in violation of s.8 of the Charter.[17]

[14] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006) [Arar inquiry, Policy Report] at 460.

[15] Government of Canada, Attorney General of Canada, *Response to Civil Claim*, in BC Civil Liberties Association v. AG of Canada, Supreme Court of British Columbia, No. S137827, 20 Jan 2014, at para. 5, on file with author.

Agency	Executive Oversight	Judicial Oversight
	and privacy-protecting measures are in place in the event that Canadian communications are captured. [16]	

1. Effective Executive Oversight

a) Concerns

One issue for Canada is how well this country manages coordinated oversight of security and intelligence operations. It is not clear to us that the minister of public safety is always able to perform that role in a satisfactory fashion. We note with concern evidence that CSIS, for instance, has not kept the minister properly informed of its activities. In its most recent annual report, it noted:

> SIRC also raised concerns regarding the mechanisms through which the Minister of Public Safety is kept abreast of pertinent developments relating to these [unnamed sensitive] activities. Although the Minister may be informed of these activities post facto through the [CSIS] Director's annual report, there is no requirement in operational policy to report on an ongoing, active basis.
>
> As SIRC noted, however, Ministerial direction requires the Director to report to the Minister, in a timely manner when there is a potential that a CSIS activity may have significant adverse impact on Canadian interests, such as discrediting the Service or the Government of Canada, giving rise to public controversy. SIRC believes that the activities reviewed often carry elements that could give rise to public controversy. Yet, SIRC found that the Minister of Public Safety is not always systematically advised of such activities, nor is he informed of them in a consistent manner. SIRC therefore recommended that CSIS strive to ensure that reporting to the Minister of Public Safety be done in a formal and systematic manner. [18]

---

[17] Forcese, Craig, Law, Logarithms and Liberties: Legal Issues Arising from CSEC's Metadata Program (March 1, 2014). Available at SSRN: http://ssrn.com/abstract=2436615 or http://dx.doi.org/10.2139/ssrn.2436615

[16] National Defence Act, s.273.65(1).

[18] SIRC Annual Report, 2013-14, at 19.

The Air India Commission was also concerned with efficacy and oversight at the executive level. It evaluated "how effectively the government uses the resources available to it to deal with the terrorist threat"[19] with particular attention to the distribution of intelligence and its relation to evidence. It recommended that CSIS should not have an unreviewable discretion to withhold relevant intelligence from others in government. Instead, the Commission recommended that intelligence should be shared and protected by a new legislated privilege from disclosure, until a decision was made by the Prime Minister's National Security Advisor about whether the intelligence should be more broadly shared within government. In essence, the National Security Advisor would perform a balancing role, deciding between the competing interests of intelligence secrecy versus its use for prosecutorial or other purposes that would risk its disclosure.

The government has shown little interest in this recommendation, one that would have increased and focused accountability at the centre of government in the interest of efficient national security decisions in the public interest. Indeed, the proposed *Security of Canada Information Sharing Act* in bill C-51 is a missed opportunity. It is a (vastly overbroad) permissive regime that may put in flow huge amounts of potentially irrelevant and unreliable information, while doing nothing to implement the Air India Commission's recommendation that some intelligence sharing be mandatory in the security interests of Canada.[20]

Indeed, bill C-51 needs to be considered against an earlier law project, bill C-44 (presently before the senate). These bills make more difficult what the Air India Commission identified as the troubled relationship between use of information for intelligence and evidence purposes. Under C-44, CSIS sources (and the CSIS Director) have a veto on whether any identifying information about CSIS's human sources can be disclosed. This will greatly complicate any subsequent reliance on evidence stemming from this source in prosecutions. By placing the veto in the hands of CSIS, C-44 prefers the interests of an intelligence agency (with a culture that gives primacy to secrecy) to the interests of police agencies (with a culture that gives primacy to investigating crimes and incarcerating criminals after a trial). [21] This decision in C-44 makes it even more important that there be effective oversight in the public interest of national security activities and in particular of the interaction between CSIS and the RCMP. Bill C-51 provides no such oversight mechanism.

There is a distressing consistency in these bills. They both reject carefully considered, fact-based commission of inquiry recommendations designed to enhance security, and instead set in train new and untested concepts that risk confounding

---

[19] Canada, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (Ottawa: Public Works and Government Services Canada, 2010) vol 3 at 1

[20] The government has provided a formal response to the report and issued a progress report but both documents are silent with respect to this critical recommendation about the enhanced role of the PM's national security advisor.

[21] Kent Roach "The Problems with the New CSIS Human Source Privilege in Bill C-44" (2014) 61 C.L.Q. 451.

successful national security strategies. For this reason, and others, we believe it unwise to assume that bill C-51 will actually increase the security of Canadians.

b) Comparative Oversight

It is worth pausing on the question of how other states manage oversight.

Other states do focus on centralized oversight. For instance, the Joint Intelligence Committee (JIC) in the UK Cabinet Office includes the heads of all three intelligence agencies as well military intelligence. It directs intelligence collection and analysis and advises the Prime Minister. David Omand who served on the JIC has stressed how the JIC's practice of formulating collective decisions lead all the members to better appreciate the other's perspective and "may be one reason why the UK has been able to work across domestic/overseas and policy/intelligence organizational boundaries on counter-terrorism...in ways that other nations with their more compartmentalized intelligence and police structures have not yet achieved."[22] If the agency heads have to co-operate and answer questions in such a committee, this should also influence all those who report to them.

There would be a case for including the highest-ranking RCMP officer with national security responsibilities in any formalized Canadian version of a JIC. And as the Air India commission recommended, there would be a need for someone independent of the agencies such as the prime minister's National Security Advisor to resolve disputes arising from the conflict between intelligence and prosecutorial priorities.

We also look with interest at developments in Australia. Australia has been contemplating closer coordination of national security agencies. Its government has recently proposed the creation of new executive counter-terrorism committee to be chaired by a national counter-terrorism co-ordinator who would be in the Attorney General's department and "build on the policy oversight of agencies" including national intelligence and financial intelligence agencies and the Australian Federal Police "which fall within the Attorney-General's portfolio. "[23] The new committee is intended "to ensure that all agencies are working in the closet possible harmony."[24] The policy review generating the rethink also defended the Attorney General playing a key and "dual hatted" role both as a law officer of the Crown concerned with propriety and legal limits on powers and as a co-ordinating Minister in the government. It stressed that counter-terrorism "needs to be more consistently whole-of-government in outlook. We must ensure all relevant government departments and agencies bring their expertise to bear. [25]

---

[22] David Omand *Securing the State* (London: Hurst, 2010) at 40

[23] Government of Australia Review of Australia's Counter-Terrorism Machinery January 2015 at 27

[24] Ibid at 22

[25] Ibid at 26

2. Limits of Judicial Oversight

The government has stressed that new CSIS powers in Bill C-51 will be subject to judicial oversight, going so far as to suggest that the new powers will be given to judges and not CSIS.

a) No Serious Prospect of Judicial Scrutiny of Information Sharing

It is critical to understand how flawed the government's assertion about judicial oversight is. First, judicial warrants are only required for a subset of activity authorized in Bill C-51. There is *no* judicial oversight contemplated with respect to the sweeping *Security of Canada Information Sharing Act*. The Arar Commission stressed the limits of courts in reviewing information sharing. It stressed that "the judiciary is a reactive institution" that can only respond to misconduct when it becomes the subject of litigation. It warned that because of secrecy "affected individuals may never know that they have been subject to a national security investigation. This reduced level of judicial oversight is a further reason for independent review." [26] Even if individuals do have such knowledge of state wrongdoing, they may not have the resources to bring a court challenge. Even if they do, they will face great secrecy barriers in their litigation.[27]

b) Judicial Warrants only Required for Some CSIS Powers

Even in relation to the new CSIS "kinetic" powers, there is no automatic judicial authorization requirement. On this question, bill C-51 specifies that the government need only seek a warrant under new s.21.1 where it has "reasonable grounds" to believe it is required. Section 12.1(3) only requires a warrant where "measures" "will" (not "may") contravene a Charter right or Canadian law. As there is no other signal on where warrants are required (and no established practice in this area, given its novelty), other measures that do not go this far presumptively do not require a judicial warrant, and the only oversight in this instance will be internal, executive branch controls.

We underscore the extent to which this means that CSIS will rarely require a warrant for its overseas operations. Canadian law is almost always confined to the territory of Canada. Likewise, the (confused) jurisprudence on when the Charter applies outside Canada suggests that it only applies where government action is in violation of Canada's international law obligations (itself a contestable and complex

---

[26] Arar Commission, Policy Report, at 491

[27] Since the Arar Commission report, the Supreme Court has made it easier for public interest groups to challenge legislation authorizing national security activities, and a group is now challenging the warrantless surveillance powers of CSE. Nevertheless such groups would still face standing challenges in challenging executive action not supported by legislative authorization and through governmental claims of secrecy. The Canadians other than Maher Arar tortured in Syria in part because of Canadian information sharing are suing Canada but their lawsuits have been delayed because of governmental claims of secrecy under s.38 of the Canada Evidence Act.

issue)[28] and (the Federal Court has suggested) that conduct is directed at a Canadian citizen.[29] Outside of these circumstances, CSIS would have no "reasonable grounds to believe" a warrant is required to police its overseas conduct.
If the government really does wish a warrant to be required for *every* measure under s.12.1, it will need to modify its language to make this intent very clear.

iii) Judicial Warrants and Procedural Shortcomings

When it is used, the Federal Court warrant regime has, in our view, one chief virtue. No Federal Court judge will ever wish to be (directly or indirectly) implicated in a scandal, court case or commission of inquiry sparked by a judge-approved CSIS "kinetic" measures gone wrong. Both personal and institutional reputations will be in play, and will encourage judicial wariness. For this reason, if we must have a warrant regime, it is better to put it into the hands of this regular court. But even with the best good will, the procedural context in which warrants are issued is a difficult one.

Role of the Federal Court

It is useful to understand how the system for conventional CSIS warrants works now at the Federal Court. At present, 14 Federal Court judges are "designated" by the Chief Justice of the Federal Court to hear CSIS warrant cases.[30] These judges typically hear CSIS applications alone.

They do, however, make efforts to coordinate activities to ensure consistency. We have recently learned that in exceptional occasions, there have been Special Sittings – that is, a sitting of a panel of judges. These have occurred, for example, when the Chief Justice considered it necessary to hear from the Director of CSIS, the General Counsel and / or CSIS personnel on procedural questions that implicated more than a single case – that is, crossover issues.

---

[28] See discussion in Forcese, Craig, Touching Torture with a Ten Foot Pole (February 2014). Osgoode Hall Law Journal (52:1), Forthcoming; Osgoode Legal Studies Research Paper No. 11/2014. Available at SSRN: http://ssrn.com/abstract=2391261. *Hape*, 2007 SCC 26 at para. 90 (concerning whether Canadian police need to observe Charter obligations while operating abroad and concluding that the Charter will not reach this conduct unless officers were "participating in activities that, though authorized by the laws of another state, would cause Canada to be in violation of its international obligations in respect of human rights"); *Canada (Justice) v. Khadr*, 2008 SCC 28 at para.2 ("The principles of international law and comity of nations, which normally require that Canadian officials operating abroad comply with local law, do not extend to participation in processes that violate Canada's international human rights obligations").

[29] Amnesty International Canada v. Canada (Canadian Forces), 2008 FCA 401; Slahi v.Canada (Minister of Justice), 2009 FCA 259

[30] Federal Court, Media Relations, personal communication, February 2015.

In these special sittings, the court has included a "neutral third party, such as a retired Justice of the Supreme Court". Should the issue arise, the latter would then be able to confirm that "the subject matter discussed was entirely appropriate".[31]

When the special sittings addressed procedural or evidentiary matters relevant to future cases, the "designated judge seized of the case proceeded to adjudicate the specific matter alone, but the other designated judges were able to obtain the benefit of the information or evidence provided during the sitting."[32]

Nature of the Warrant Process

This close coordination is important because of the secretive nature of the warrant proceedings. CSIS warrant proceedings are *ex parte* and *in camera*. That means that they are held in closed court, with only the government side represented. This is typical for all warrant applications – there would be no logic to a system in which the target of a covert surveillance operation would be apprised of that operation in order to make representations on whether it should be authorized.

Nevertheless, it is important to underscore the consequence of this one-sided process. Our system of justice typically depends on an adversarial process in which judges weigh the views of two sides, each with an incentive to set out thoroughly its position. Commenting on another type of *ex parte* proceedings Justice James Hugessen stated in 2002 that judges "greatly miss… our security blanket which is the adversary system that we were all brought up with and that…is for most of us, the real warranty that the outcome of what we do is going to be fair and just."[33]

One safeguard in an *ex parte* proceeding is a firm requirement that the government by perfectly candid with judges. It must bring all relevant information to the judge's attention. We believe that the government is generally observant of this firm obligation. However, there are instances where it has breached this duty. There are now several Federal Court decisions complaining that CSIS has failed to meet its duty of candour in closed door proceedings.[34] It is very difficult to know whether these reports represent the sum total of CSIS shortcomings – a failure to be candid is something that is, by definition, very difficult to detect.

---

31 *Ibid.*

32 *Ibid.*

33 James K. Hugessen, "Watching the Watchers: Democratic Oversight" in David Daubney *et al.*, eds., *Terrorism, Law and Democracy: How is Canada changing following September 11?* (Montreal: Canadian Institute for the Administration of Justice, 2002) 381 at 384-385.

34 See, most famously and recently, *Re X*, 2014 FCA 249. Candour issues also have characterized several of the immigration "security certificate" cases. See, e.g., *Almrei (Re)*, 2009 FC 1263.

Moreover, even with the best good will, the fact is that any agency will be vulnerable to "group think" and tunnel vision. It is exactly these kind of phenomena that underlie many miscarriages of justice in Canadian history.[35]

The Federal Court may try to mitigate the risks associated with ex parte proceedings by enlisting the assistance of a "friend of the court" or *amicus curiae* to restore a quasi-adversarial system. Such an approach in the warrant context is an approximation of the "special advocate" role in the famous immigration security certificate proceedings, itself the product of constitutional requirements set down by the Supreme Court after a lengthy judicial process.[36]

It is important to recognize, however, the extent to which a CSIS warrant process differs even from the imperfect situation under a security certificate. First, under the security certificate process, "special advocates" are a statutory office with statutory roles and responsibilities. That places them in a significantly more meaningful role than is the case with *amici*. Indeed, a recent Federal Court decision suggests that the role of *amici* in *ex parte* proceedings where vary depending on the judge's predispositions and may be more limited than that of a special advocate.[37]

Second, although underfunded, special advocates are at least supported by a special support unit, organized at arm's length from the Department of Justice. *Amici* do not benefit from this administrative structure and at best operate in splendid isolation, with only the resources they can personally bring (and which do not include assistance from their own firms for security reasons, if not other) or which the court itself provides.

Third, *amici* have no independent standing to bring, e.g., appeals. In the result, warrant decisions are unappealable by any party other than the government.

Four, whatever the imperfections of the immigration security certificate process, at least there is a "named person" aware that their interests are being adjudicated and able to provide information to the special advocate. Indeed, after the *Harkat* decision of the Supreme Court,[38] there is a presumption in favour of ongoing communication between special advocate and named person, subject to care that the special advocate disclose no secret information.

---

[35] Tunnel vision or confirmation bias including a focus on a unpopular and odd suspect has contributed to many miscarriages of justice (ie. Donald Marshall Jr., David Milgaard, Guy Paul Morin etc) even when the police know that their investigation will be subject to adversarial challenge in court. It is perhaps even more likely in intelligence operations and in legal contexts without full adversarial challenges. See Kent Roach and Gary Trotter "Miscarriages of Justice in the War Against Terror" (2005) 109 Penn.State. L. Rev. 967.

[36] Charkaoui v. Canada [2007] 1 S.C.R. 350.

[37] Canada (Procureur général) c. Telbani, 2014 CF 1050

[38] Canada (Citizenship and Immigration) *v.* Harkat, 2014 SCC 37

The presence of a named person able to feed information to the special advocate is critical to the latters' effectiveness – there is a source of information other than the government, and inconsistencies and contradictions in the government's position may be made obvious and then adjudicated by the court.

None of these qualities exist in the CSIS warrant context. It would wrong, therefore, to imagine that an *amicus* can correct all the shortcomings of the *ex parte* an *in camera* process.

We note that the United States Privacy and Civil Liberties Oversight Board condemned these same sort of procedural shortcomings – secretive authorizations, absence of appeals, and no robust special advocate system – in a recent review of the US "FISA" Court. In a report on National Security Agency (NSA) collection of metadata that questioned the NSA's interpretation of the legal authorization for the collection of such material, the Board was critical of US oversight in the area of surveillance by the US "FISA" Court and recommended that special advocates be able to appear before the court; that appeals of the FISA's court decisions be facilitated; and that more appeals be declassified. [39]

Absence of Retrospective Scrutiny

Nor should anyone assume that CSIS warrants can be challenged retrospectively. CSIS warrants, unlike Criminal Code warrants, are not designed to produce evidence that can be tested in criminal trials and appeals. CSIS investigations only become the subject matter of trials in very rare circumstances, and even then there are usually procedural disputes as to what and whether CSIS must reveal much about its conduct. We observe here that for these sorts of reasons, the Arar Commission noted that the comparative lack of prosecutions in the national security area means that the courts provide "less oversight" than national security investigations "than they do for other criminal investigations.[40]

Moreover, police surveillance authorizations under Part VI of the Criminal Code must be disclosed to the target after the passage of time, and subject to extensions. CSIS warrants are never disclosed. All of this is to say that CSIS warrants are and remain secret.

Finally, there is no true "feedback" loop to the judge issuing a CSIS warrant allowing her or him to scrutinize what CSIS purports to do pursuant to the warrant and the actual terms of that warrant. What is authorized and what is done by CSIS may not

---

[39] Privacy and Civil Liberties Oversight Board Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court, Jan 23, 2014 available at https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf. See also Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated under s.702 of the Foreign Intelligence Surveillance Act July 2014 at 146.

[40] Arar Commission, Policy Report, at 439

always corresponded, as a recent Federal Court decision suggests.[41] There, the Court only learned of the gap between a security intelligence warrant authorization and CSIS conduct through an accident. A particularly earnest judge reviewing a public SIRC report and the public report of the CSE commissioner noted inconsistency between the practice attributed to his warrant and the actual content of the warrant.

This should not be taken as good evidence that the accountability system "works". It is, at best, a form of "fortuitous accountability". The system "worked", but by happenstance and not design. Indeed, the SIRC and CSE commissioner report betrayed a misunderstanding of what the judicial warrant actually prescribed. It would appear that no one had audited the actual content of the warrant against the CSIS conduct, and the judge who knew the content of the warrant only learned of the conduct because it happened to be reported (and incorrectly described as actually authorizing the activity in question) in the review body report.

The absence of formalized, standing "feedback" loops between authorizing judges and review bodies is one of the many striking omissions in the Canadian national security accountability system. It is one thing not to have feedback loops where all that is at issue is covert surveillance. It is quite another where the entire range of Charter rights may be at issue, as bill C-51 seems to suggest. But even a perfect feedback loop would have disadvantages because it would slowly move judges in our adversarial system towards a model of investigating magistrates found on the European Continent. We acknowledge that some may prefer such a system, but it has not been our system, and our judges are not trained or equipped for this task.

We believe that Federal Court judges may nevertheless contemplate structuring these feedback loops by creating more formal links with SIRC. Under proposed s.21.1(5)(f), judges may impose "any terms and conditions that the judge considers advisable in the public interest". It is our hope that judges would consider correcting deficiencies in the area of formalized feedback loops by imposing a requirement that the minister request a special review by SIRC under s.54(2) of the CSIS Act of CSIS's performance under the warrant at issue. Such an approach would ensure a "follow through" that we fear might otherwise not exist. We recognize, however, that placing such "judicial mandates" on SIRC will increase the formidable challenges that SIRC already faces. We will discuss some of these challenges below.

3. Parliamentary Role in Oversight

Before turning to "review" we address the issue of oversight and legislative bodies. Recall what we mean by oversight: command and control.

Legislative bodies do not do true oversight – that is, they do not authorize operations. It is true that in the United States, the executive notifies some legislators of at least some security operations (particularly covert operations).[42]

---

[41] *Re X*, 2013 FC 1275.

[42] See Eric Rosenbach, *Confrontation or Collaboration? Congress and the Intelligence Community* (Intelligence and Policy Project of Harvard Kennedy School's Belfer Center for Science and

United States law provides: "The President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity".[43] In this respect, the US Congress straddles a relatively unique position as a review and accountability body that also is privy to close to real time operational information. As we understand it, Congress does not, however, actually approve or supervise operations, and thus does not perform "oversight" in the sense this term is used in Canadian practice.

Australia, a state with a Westminster system very similar to Canada's, also incorporates a requirement that the executive apprise at least some legislators of key operations. The statute governing the Australian Security Intelligence Organization (ASIO), Australia's CSIS equivalent, provides: "The Director-General [of ASIO] shall consult regularly with the Leader of the Opposition in the House of Representatives for the purpose of keeping him or her informed on matters relating to security."[44]

Notably, however, there are circumstances in other countries where *individual* parliamentarians may be implicated in *true* oversight. This arises with "hybrid" parliamentary and expert bodies. In Germany, an expert body whose members can include parliamentarians performs an oversight role roughly equivalent to that conducted by courts in Canada. Specifically, the G10 Commission has the power to authorize surveillance measures that invade privacy protections. The members of this commission are elected by the German parliament's special "parliamentary control panel", a body charged with scrutinizing the German intelligence services.[45]

Likewise, Sweden's Commission on Security and Integrity Protection (Swedish acronym "SIN") also may perform an oversight role in relation to ongoing operations. Like the G10 Commission it includes experts but may also include legislators. Swedish lawmakers created SIN in 2007 for these reasons:

> [i]ncreased investigative powers had been, or were in the process of being, granted to the police and the Security Police. There was also a realisation that prosecutorial and judicial control only checked if there was reasonable cause to initiate surveillance, and there was no post hoc monitoring. SIN was thus given a follow-up oversight function over surveillance.[46]

International Affair), online: http://belfercenter.ksg.harvard.edu/publication/19148/informing_congress_of_intelligence_activities.html

[43] 50 U.S. Code § 3091.

[44] Australian Security Intelligence Organisation Act 1979, Act No. 113 of 1979, as amended, s.21.

[45] Wills et al, above note 3 at 218.

[46] *Ibid* at 280.

The Swedish decision seems particularly instructive. As discussed above, Canada also suffers from the absence of formal "feedback" loops linking judicial authorizations to actual conduct under a CSIS warrant.

B. The Concept of Review

In the absence of robust "feedback" loops for oversight mechanisms, we are dependent on robust "review". Indeed, even with such feedback mechanisms, we underscore again that judicial oversight would only relate to a fraction of the activities undertaken by the security services. For this reason also, we are all the more dependent on robust "review".

1. Basic Principles

Examining review mechanisms for national security agencies was the key preoccupation of the Arar inquiry's policy phase, and that commission's analysis represents the most comprehensive treatment of this issue in Canadian history.

The Arar report enunciated several key considerations favouring a robust review mechanism for security and intelligence bodies. National security activities

> involve the most intrusive powers of the state: electronic surveillance; search, seizure and forfeiture of property; information collection and exchange with domestic and foreign security intelligence and law enforcement agencies; and, potentially, the detention and prosecution of individuals. The use of such powers may adversely affect individual rights and freedoms.[47]

Unlike regular criminal investigations, however, national security matters are deeply surreptitious and secret. The writ of Canada's information access laws usually stops short of national security matters. Those who have been investigated may be eternally oblivious to this fact, and in no position to complain about misconduct. Indeed, if no charge is laid and no decision is made to commence a prosecution, none of the investigation undertaken by the authorities will ever be tested before an impartial decision-maker.

Even where courts are implicated, that review may be attenuated, curtailed by special secrecy or other rules that constrain the full expression of the adversarial system on which Canadian justice is predicated.[48] Parliament, meanwhile, has a traditionally limited role in security and intelligence review, a point explored more fully below.

For all these reasons and more, the national security structure lacks many of the checks and balances deemed essential in other aspects of Canadian political and legal life. Absent these constraints, the proper functioning of national security agencies

---

47 Arar Commission, Policy Report, at 425–26.

48 Ibid.

depends heavily on the integrity of those who populate it. There is no reason to doubt that integrity on an individual level. Every bureaucracy suffers, however, from its own shortcomings, some serious. A bureaucracy immune to external scrutiny may find it difficult to resist the temptation to stretch uncertain boundaries. It may also stray into patterns, policies or group-think impairing its effectiveness.

These considerations all counsel effective review mechanisms – audits and complaint systems able to measure agency compliance with legal or other standards and query problematic behaviour. National security law expert and government lawyer Stanley Cohen aptly captures the standard to be applied in national security review: trust, but verify.[49]

2. Elements of Effective Review

Designing a review mechanism to accomplish these goals presents important challenges. Academic experts view effective review as resting on several design elements.

- First, review must be conducted by a body that is independent of the government and the agencies that it reviews. The body is not, in other words, both the watcher and the watched.

- Second, this body must be mandated to audit, review and assess the legitimacy of security intelligence actions.

- Third, it must have real powers to review and investigate at its discretion, compel and examine even secret information, respond (and propose resolutions) to public complaints, make public reports of its findings and conclusions, and have in place a means to protect and secure confidential information.[50]

The Arar inquiry proposed its own, similar list of design criteria.

- First, review should ensure compliance with national and international law and "standards of propriety that are expected in Canadian society."[51]
- Second, it should enhance accountability of security and intelligence agencies to the government, and ultimately Parliament and the public.
- Third, by enhancing accountability, a review system should encourage public trust and public credibility of the agency. To achieve this goal, it should be

---

49 Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, ON: LexisNexis Butterworths, 2005) at 561.

50 See Ottawa Principles on Anti-terrorism and Human Rights (2006), Principle 9.3 [on-line].

51 Arar inquiry, Policy Report at 502.

> independent and staffed in a transparent manner by qualified individuals. It should also disclose, as much as possible, details of its actions and findings.[52]

The Arar Commission stressed that any credible review mechanism for propriety should have unrestricted access to secret information and the ability to initiate its own audits or investigations. It was not opposed to review bodies also adjudicating public complaints, but recognized that limits of such mechanisms as a tool of accountability given the secrecy of much national security.

More recently, the United Nations Special Rapporteur on the "promotion and protection of human rights and fundamental freedoms while countering terrorism" tabled a report in the UN Human Rights Council compiling "good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight" (Scheinin report).[53] He addressed review and accountability. He urged that at least one accountability agency should be a civilian body independent of both the intelligence service and the executive" and the remit of the institutions should cover "all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices."[54] The report also recommended that accountability "institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates."[55] Intelligence services should cooperate fully with these bodies in providing witnesses, documentation and other evidence.[56]

At the time of this writing, Canada's security intelligence review mechanisms were variable in their structure and performance and uneven in their distribution. The Arar inquiry recommended reforms that would radically change this landscape. With the exception of reforms to the RCMP review body that fall short of the actual Arar recommendations because they do not guarantee that the reviewer will have access to secret information, none of structural changes have come to pass.

Part II: Review in Canada

A. Overview

There are only three national security review bodies in Canada: the Security Intelligence Review Committee (SIRC), for CSIS; the Commissioner of the

---

52 *Ibid*.

53 United Nations Doc. A/HRC/14/56 (16 May 2010).

54 Scheinin Report, Practice 6 at 8.

55 *Ibid*, Practice 7 at 9.

56 *Ibid*.

Communications Security Establishment; and (to a lesser degree), the RCMP Civilian Review and Complaints Commission. There are a few agencies with vary narrow and specific mandates who perform "all-of-government" review – the Privacy Commissioner (for privacy) or the Auditor General (for financial management). But these bodies have neither the mandate nor the expertise to assess national security operations per se. The Privacy Commissioner underlined most recently in a 2014 that its powers were not up to the task of reviewing information sharing in the security context. [57]

There are no national security review bodies for the many other Canadian government agencies implicated in bill C-51. The "whole of government" approach to security is epitomized in the proposed *Security of Canada Information Sharing Act* that would allow any federal institution to share security information with 17 different departments. Again, only three of these bodies (CSIS, CSEC and RCMP) are subject to national security review. For instance, CBSA performs both law enforcement and intelligence functions. It is subject to no independent review. Indeed, as best we know, it is the only law enforcement body in Canada not scrutinized by a review body or a police services board of some sort. Review of this CBSA body is sporadic: for instance, occasional coroner's inquires, when persons in its custody die.[58] In the current Parliament, a private members bill – S-222 sponsored by Senator Moore – proposes an inspector general for CBSA. We assume that as with virtually all private members bills, its prospects are dim.

Put simply, the review system in Canada is "stovepiped" – review bodies are empowered to review only their specific agencies. They are legally limited in their ability to coordinate investigations and reviews — as we understand it, the government has even suggested that coordination would violate Canada's criminal law on secrecy.[59]

For exactly this reason, and as we discuss below, a key recommendation of the Arar commission was closer links between the review bodies, allowing more coordinated pursuit of reviews. Another important recommendation was the expansion of the number of government agencies subject to some sort of review.

None of these changes have ever been made, despite the passage of almost 10 years, an acceleration of security agency integration, and repeated reports – including by SIRC itself – on the extent to which review in Canada in conducted under increasingly unsustainable circumstances.

---

[57] Canada. Office of the Privacy Commissioner of Canada, Checks and Controls Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance (Ottawa: Minister of Public Works and Government Services Canada, 2014)

[58] James Keller, "BC coroner inquiry called after CBSA airport detainee death," Canadian Press (Feb 25, 2014), online at http://metronews.ca/news/victoria/953041/b-c-coroner-inquest-called-after-cbsa-airport-detainee-death/.

[59] Colin Freeze, "Spy agencies try to curb watchdogs' ties to each other," *Globe and Mail* (May 29, 2014), available at http://www.theglobeandmail.com/news/national/spy-agencies-try-to-curb-watchdogs-ties-to-each-other/article18919190/#dashboard/follows/.

Bill C-51 increases the powers of CSIS considerably – it is the most important change ever made to CSIS in its history. In comparison, the only language on review included in C-51 says: "In reviewing the performance by the Service of its duties and functions the Review Committee shall, each fiscal year, review at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada". [60]

In other words, not every kinetic measure that CSIS will now undertake, possibly pursuant to a warrant allowing it contravene the law or Charter, will be scrutinized – we are in the area of partial audits of potentially only one of the many "aspects" of CSIS actions under the broad kinetic power system.

B. SIRC in Context

1. Past Academic Assessments

Canada's system of review predates many of the developments undertaken by other democracies in relation to their own security intelligence sector. As a consequence, Canada – and particularly its SIRC – is sometimes viewed by these counterpart agencies with considerable respect. Within Canada, however, the CSIS review agency has a low profile, and has attracted attention recently mostly because of the notoriety of its former chair, Arthur Porter (currently in prison in Panama).

There is very little written in the public domain on review in Canada. We provide a brief bibliography.

Several (now dated) academic articles have been authored by former SIRC members or employees, and explain features of SIRC's operations[61] or, in one case, defend it from criticism.[62]

Perhaps the most comprehensive assessment of SIRC dates to a 1989 academic article in which UK security intelligence expert Peter Gill reviewed the impact of SIRC during the period 1984-1988.[63] Gill probed SIRC's performance with an eye to four questions: 1. Did SIRC have adequate resources? 2. Did SIRC have the will to use these resources energetically? 3. Can SIRC obtain the information necessary for effective review? 4. Measured by its impact on CSIS performance, does SIRC have political influence?

---

60 Bill C-51 Part 4 adding s.38(1.1) to the CSIS Act

61 See, e.g., J.J. Blais, "The political accountability of intelligence agencies Canada," (1989) 4:1 *Intelligence and National Security* 108; Murray Rankin, "National Security: Information, Accountability, and the Canadian Security Intelligence Service," (1986) 36:3 *University of Toronto Law Journal* 249.

62 Maurice Archdeacon, "The heritage front affair," (1996) 11:2 *Intelligence and National Security* 306.

63 Peter Gill, "Symbolic or real? The impact of the Canadian security intelligence review committee, 1984–88," (1989) 4:3 *Intelligence and National Security* 550.

Gill's assessment was largely positive. He rejected the notion that SIRC had been intentionally under-resourced. While SIRC's work was largely reactive, responding to matters brought to its attention, it had produced important proactive reports. Notably, this success was regarded as a "beneficial spinoff from the appeals process into review and in part also because SIRC has been able to make use of the Inspector General's resources by tasking him under s.40 to carry out reviews".[64] As noted below, the Inspector General no longer exists.

Gill also commented favourably on SIRC's propensity to publicize its criticisms of CSIS, regarding this as evidence of a will to have a real impact. Gill regarded this public exposure – more than any particular originality in SIRC's analysis – as an important driver of change at CSIS. He also assessed SIRC's access to sufficient information as real. Finally, Gill drew some provisional conclusions about SIRC's impact on CSIS, discerning some changes that he attributed to SIRC's scrutiny.

Gill's assessment of SIRC may constitute the high water mark. Academic assessments thereafter have been more critical, if less systematically comprehensive. In 1992, York University political scientist Reg Whitaker acknowledged that "very significant public presence" of SIRC during its first five year, under the stewardship of its first chair, Ron Atkey.[65] Whitaker observed that SIRC had not yet been co-opted by the agency it was charged to review, a perennial threat to SIRC-like institutions. At the same time, he warned that Canada was entering an era of policy drift and institutional inertia, and only public scandals were likely to shake this inertia.[66]

In a subsequent 1996 article, Whitaker assessed SIRC's performance during the 1994 "Bristow case". He concluded that "[a]lthough SIRC has fulfilled most of the implicit expectations of the government in the affair, it has by no means emerged unscathed. ...[T]he spotlight cast upon the review body's unrepresentative political make up...have done it some lasting harm".[67]

More recent academic articles have commented on SIRC's modest funding, describing them as out-matched by increased CSIS resources.[68] Meanwhile, in an opinion piece written in 2002 on the aftermath of 9/11, Wark observed that "SIRC has been invisible and silent since Sept. 11. It failed to undertake an immediate

---

64 *Ibid* at 570.

65 Reg Whitaker "The politics of security intelligence policy making in Canada: II 1984–91," (1992) 7:2 *Intelligence and National Security* 53 at 59.

66 *Ibid* at 72.

67 Reg Whitaker, "The 'Bristow affair': A crisis of accountability in Canadian security intelligence," (1996) 11:2 *Intelligence and National Security* 279 at 301.

68 Roy Rempel, "Canada's Parliamentary Oversight of Security and Intelligence," (1994) 17 *International Journal of Intelligence and CounterIntelligence* 634 at 638.

review of Canadian security intelligence knowledge surrounding the attacks, one more sign that SIRC has lost its early edge."[69]

b. Contemporary SIRC Review

We turn now to a more contemporary overview of SIRC's composition, functions, and challenges.

1. Staffing

The Security Intelligence Review Committee (SIRC) has up to five parttime "members" supported by a small staff. The members of SIRC are appointed by the governor-in-council (after consultation with the leaders of official parties in the Commons) for five-year terms, and sworn into the Queen's Privy Council for Canada. The posting is a part time one, with SIRC members meeting periodically (which we understand to be about 5-6 times) during the year.

The SIRC membership has often been understaffed during recent years. Until recently, it stood at three. When bill C-51 was tabled in Parliament, the Prime Minister announced the appointment of a fourth member, Dean Ian Holloway of the Faculty of Law, University of Calgary. A vacancy still remains to be filled before SIRC is at full complement.

2. Budget

In 2014 SIRC was staffed by an Executive Director and 17 staff members, and had expenditures totalling $2,901,300,[70] a tiny fraction of CSIS's operational budget, and proportionally smaller than through much of its history.

One of us attempted to paint a statistical portrait of SIRC's financing in 2012 that included data from SIRC's beginnings through fiscal 2010.[71] SIRC funding has always been modest relative to that of CSIS. Between 1985 and 2009, it averaged 0.77% of CSIS funding. At certain periods – especially in the early 1990s – it fell well below this level, before moving back to average or above-average figures in the early 2000s. In 2004, it rose to its highest level ever – 0.97% of CSIS funding – after a 2002 request from SIRC that its funding be increased to reflect the increased size of CSIS post-9/11.[72]

---

[69] Wesley Wark, "Our security IQ needs testing," *Globe and Mail* (28 Feb 2002) A19.

[70] Security Intelligence Review Committee, *Annual Report 2013-2014*, p 34-35, available online: http://www.sirc-csars.gc.ca/pdfs/ar_2013-2014-eng.pdf.

[71] Forcese, Craig, The Social Cost of National Security Symposium: Accountability with a Pinch of Context and a Dash of Fire and Brimstone (October 1, 2012). (2012) 91 Canadian Bar Review 1. Available at SSRN: http://ssrn.com/abstract=2551295

[72] See discussion in Canada, SIRC Annual Report, 2004-2005, at http://www.sirc-csars.gc.ca/anrran/2004-2005/sc03-eng.html#s2.

More recently, however, SIRC spending fell to the lowest levels of its history, relative to that of CSIS. In 2008-2009 and 2009-2010, SIRC spending was 0.56% and 0.51% of CSIS spending. (Notably, calculations for CSIS spending for 2009-2010 subtracted the $44 million spent on the new CSIS headquarters for that year and so can be regarded as capturing only spending on personnel and operations.)[73]

Developments since 2010 suggest that the situation has become worse.[74] CSIS's budget for the most recent annual report period posted on its website (2011-2012) was $540 million.[75] SIRC's budget during the same period was $2.57 million, or 0.5% of the CSIS budget. This would appear to be the worst relative funding level between SIRC and CSIS ever witnessed during CSIS's history.

The 2014-15 estimates place CSIS's budget at $516 million and SIRC at $2.8 million, or 0.54% of the CSIS budget.[76] While not as abysmal as earlier in this decade, this figure remains below historical levels.

SIRC has identified funding issues as a challenge in the past. In June 2007, before the Standing Senate Committee on National Security and Defence, former Excutive Director Susan Pollak commented on the bureaucratic constraints placed on SIRC. When asked about whether the small size of the committee and the scope of its mandate was a challenge, the Director responded:

> Yes, and it is even more of a challenge these days because SIRC is a public agency and, of necessity, we have to abide by all of the same reporting mechanisms that others do, but I can tell you that between the management accountability framework and the management of information technology strategy and the program activity architecture, there is this burgeoning group of reporting mechanisms coming at us fast and furiously; ... It is taking a lot of our time. We were not funded to deal with quite as much as is in play today.[77]

---

[73] Data for these calculations were collected from the SIRC and CSIS annual reports available on the website of these organizations. SIRC annual reports report CSIS budgets throughout the 1980s and into the 1990s. The period for which data on CSIS budgets were available was 1985-2009.

[74] Chris Hall, CBC, CSIS watchdog agency starved of staff, resources (Feb 20, 2015), online: http://www.cbc.ca/news/politics/csis-watchdog-agency-starved-of-staff-resources-1.2965276.

[75] CSIS Annual Public Report, 2011-2013, on line: https://www.csis.gc.ca/pblctns/index-en.php?cat=01.

[76] Treasury Board of Canada, 2015-16 Estimates, http://www.tbs-sct.gc.ca/ems-sgd/me-bpd/20152016/me-bpdtb-eng.asp

[77] Canada, Parliament, Senate, Standing Committee on National Security and Defence, *Evidence,* 39 Parl, 1st Sess, (18 June, 2007) available online: http://www.parl.gc.ca/Content/SEN/Committee/391/defe/17evb-e.htm?Language=E&Parl=39&Ses=1&comm_id=76.

3. Access to Secret Information

Under the CSIS Act, SIRC has broad rights to CSIS information.[78] It may not see Cabinet confidences, but it does regularly see data supplied to CSIS by foreign governments and agencies.[79] Members of SIRC and its employees must comply with all security requirements under the CSIS Act and take an oath of secrecy.[80] They are also "persons permanently bound to secrecy" under the *Security of Information Act*, and are therefore subject to that statute's penalties for wrongful disclosure of sensitive information.

Despite these legal powers, there have been occasions where SIRC feels it has been misled by CSIS, and not given full access to information. In the 2013-2014 Annual Report, SIRC outlined its investigation into a complaint where if was found:

> that SIRC had been seriously misled by CSIS on this same point. SIRC found that CSIS had violated its duty of candour during ex parte proceedings by not proactively disclosing in its evidence not only its rejection of the reliability of the source of information, but also the falseness of some allegations against the complainant. A witness had to be recalled by SIRC to speak to the matter and SIRC found CSIS's lack of candour most disturbing. The investigation revealed further examples of inadequate assessment of the complainant's activity. It also revealed that the written reports derived from the complainant's security screening interviews provided an inaccurate portrayal of the complainant's interview answers, which SIRC was able to ascertain by obtaining the original audio recordings.[81]

In the same report's "Message from the Committee" it was also noted:

> In two reviews, SIRC encountered significant delays in receiving requested documentation and had to press the Service to obtain complete and consistent answers to several questions. With effort, SIRC was eventually provided all the relevant information it required to carry out and complete its reviews, but these difficulties and delays caused the Committee concern.
>
> SIRC encountered similar disclosure difficulties in the investigation of two complaints. In one investigation, SIRC found that it had been seriously misled by CSIS and that CSIS had violated its duty of candour during ex parte proceedings by not proactively disclosing in its evidence its rejection of the reliability of a source of information. In a second complaint report, SIRC was critical of CSIS for failing to proactively highlight a highly relevant document. SIRC reminded CSIS that its disclosure obligations went

---

78 CSIS Act, subs. 39(2).

79 Arar inquiry, Policy Report at 278.

80 CSIS Act, s. 37.

81 Security Intelligence Review Committee, *Annual Report 2013-2014*, at p 27-28, available online: http://www.sirc-csars.gc.ca/pdfs/ar_2013-2014-eng.pdf.

> beyond producing a large quantity of documents for SIRC's review and included the duty to proactively present the most relevant pieces of evidence before any presiding Member.[82]

In his message, the Executive Director echoed the Committee's concerns:

> SIRC has often described its relationship with CSIS as one of "healthy tension." Indeed, while we strive to maintain a cordial and professional relationship with our CSIS counterparts, our foremost objective is always to ensure that we receive all the relevant information we require to effectively carry out reviews and complaints investigations.
>
> This past year, SIRC encountered challenges in this respect; in some instances, I had to personally intervene to ensure that staff received complete information. Having brought these issues to the attention of the Service's senior management, I am confident in CSIS leadership's ability to take the necessary steps to resolve the situation.[83]

5. Review Functions and Difficulties

SIRC is tasked with, among other things, reviewing the performance by the Service of its duties and functions.[84] (SIRC also has a complaints function that we do not discuss further here).

It should be underscored that SIRC's review of CSIS activities has always been partial – it does not and cannot review every activity. For instance, SIRC has explicitly stated that it does "not have the resources to examine all warrants granted to the Service" even in the present surveillance-only system. Instead, it "look[s] at a certain number of warrants as part of its annual review activity."[85] Put more generally, it samples, reviewing seven or eight review topics per year. (Since the abolition of the Inspector General, discussed below, one of these reviews must involve certifying that the CSIS director's report to the minister is sound, meaning that there are even fewer unique reviews done now than before).

In its *2011-2012 Annual Report*, SIRC noted (obliquely) how it tries to mitigate the risk of this partial approach:

> SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and activities. The Committee's research program is designed to address a broad range of subjects on a timely and topical basis.....Each review results in a snapshot of the Service's actions in a specific case. This approach allows SIRC to manage the risk inherent in

---

82 SIRC, *Annual Report 2013-2014*, p 3.

83 SIRC, *Annual Report 2013-2014*, p 7.

84 CSIS Act, s. 38.

85 SIRC, *2006-2007 Annual Report*, at 52.

> being able to review only a small number of CSIS activities in any given year.[86]

Under the CSIS Act, the outcome of the SIRC investigation is conveyed to the minister and the CSIS director, along with SIRC's recommendations. SIRC recommendations are not binding on the government.[87]

SIRC also has more general reporting functions. It prepares special reports where requested by the minister or at any other time[88] and an annual report, tabled by the minister in Parliament,[89] which in practice contains summaries of the committee's investigations.

Review Spread More Thinly and By Increased CSIS Foreign Operations

Bill C-51 will increase dramatically the sort of activities that CSIS may undertake. SIRC will need, therefore, to continue its review of CSIS's conventional intelligence operations, while now also diverting attention to review of CSIS's "kinetic" operations. The modest number of reviews SIRC can currently conduct will be spread over a greater range of activities. SIRC, underresourced at present, will be spread even thinner, meaning that it may be hard pressed to maintain its current level of scrutiny of intelligence operations while at the same time hard pressed to truly review CSIS's kinetic conduct.

This problem will be greatly acerbated by the fact that both bills C-44 and C-51 now clearly permit CSIS overseas operations. In essence, just as CSIS's powers are being expanded, so to is its geographic range. The implications of creating a "foreign intelligence service" in this haphazard manner are considerable and deserving of their own close scrutiny. Buried in these two bills, this creeping foreign intelligence service has attracted virtually no serious discussion, except by Professor Wesley Wark during testimony on bill C-44.[90]

The prospect of a resource strained, understaffed review body now being obliged to extend its reach into (expensive) extraterritorial reviews that now involve not just intelligence gathering but "kinetic" activities is daunting and gravely concerning. In addition, it can be expected that when acting outside of Canada, CSIS will work closely with the Department of Foreign Affairs and the Department of Defence, as was the case in Afghanistan. SIRC will have no jurisdiction to examine these latter department or anyone other than CSIS.

---

86 *Ibid*, p 9.

87 Thomson v. Canada (Deputy Minister of Agriculture), [1992] 1 S.C.R. 385.

88 CSIS Act, s. 54.

89 CSIS Act, s. 53.

90 House of Commons Standing Committee on Public Safety and National Security (November 26, 2014).

"Stovepiped" Review

In this last respect, SIRC's review functions are confined to CSIS, a "stovepiping" that SIRC itself has questioned. In its 2012-2013 Annual Report, SIRC addressed the increased information sharing between government and foreign agencies:

> As the technological barriers between information systems and previously stove-piped databases continue to fall, the sharing of data has become not merely possible, but routine. In the material explored in this annual report, we examine how there are both advantages and risks in this development, and we will highlight the growing challenges for their complete and effective review.
>
> As CSIS moves to take advantage of this new capacity, SIRC must also be able to respond. It must be flexible enough to follow up and effectively review CSIS activities and investigations, even when they cross over with other agencies and departments. Given the inevitability of technological interconnectivity, SIRC must be ready with the legislative tools and matching government resource commitments to ensure that the checks and balances enshrined in the Committee remain relevant and effective.[91]

Parliament has enacted no new legislative tools, although the government has reportedly been considering this question for years.[92]

In 2013, before the Senate Committee on National Security and Defence, Chuck Strahl, then Chair of SIRC, was asked about co-operation between the review agencies of CSIS and CSE. He noted:

> neither of us has clearance to delve into the details of the other's operation. Both committees have issued reports saying, in essence, that we need to work together more, and it is reflective of what was said in Justice O'Connor's report and Justice Iacobucci's report and others that said there needs to be some way. One suggestion was there needs to be a statutory gateway into one another's world so you can get into the details when necessary. I think both of us feel somewhat — I don't know if the word is frustrated — but certainly inhibited. We are very cautious. If the legislation is clear that we're allowed to go and look at everything that CSIS does, but there's no mention of CSEC, well, then we do everything that CSIS does....
>
> I think there is increasing understanding that our worlds overlap quite a bit and that we need to find better ways for both of us to get into the weeds when we need to, if I can use the expression, because once in a while, the trail is not going to stop nicely and neatly at CSIS's door. It blends not just

---

[91] Security Intelligence Review Committee, *Annual Report 2012-2013*, p 10, available online: http://www.sirc-csars.gc.ca/pdfs/ar_2012-2013-eng.pdf.

[92] Jim Bronskill, "Work on better spy monitoring still underway four years after promise: feds," *Hamilton Spectator* (Feb. 26, 2015).

> into CSEC but also others. Other agencies, by necessity nowadays, are working closely with CSIS, and increasingly we're going to need some way of chasing those threads. Otherwise, we'll have to tell parliamentarians that, as far as we can tell, everything looks great in CSIS country, but we don't know what happened over that fence; you're on your own.

Also 2013, before the Senate Committee on National Security and Defence, Mr. Strahl, outlined SIRC's research into the matter of Mr. Abdelrazik, a Canadian who had been repeatedly foiled by the Canadian government in efforts to return to Canada after maltreated in Sudan.[93] The Chair emphasized that this review:

> did underscore SIRC's limitation to follow information when it crossed over to other federal departments or agencies. For a number of years, SIRC has been saying that although it has great powers to review CSIS's activities and operations — all the powers I mentioned earlier — this ability does not extend beyond CSIS. As even greater integration and information sharing becomes the modus operandi of contemporary intelligence work, SIRC believes it should be equipped with the tools needed to follow and effectively review CSIS's activities. As we say in our annual report, SIRC must be ready with the legislative tools and matching government resource commitments to ensure that the checks and balances enshrined in its mandate remain relevant and effective.[94]

He further stated:

> What we're finding increasingly is that CSIS is having to engage other partners in order to get the information they want. We can examine anything that CSIS does. What we have highlighted and made note of is that we are increasingly nervous or wary of the fact that you come up to an imaginary wall, if you will, where we examine everything that CSIS does, but now it involves other departments. It might involve a no-fly list. It might involve CBSA or CSEC, and so on, but our authority extends only to CSIS in our review process. So I think the committee is, and the government would be, wise to look at — and it's a modern reality — how we can make sure that we don't, when we're chasing a thread and trying to make sure that Canadians' rights are being protected, run up into the legislative wall of saying, "Well, yes, but you can only look at CSIS, even if the new thread continues on into CSEC," as an example. That is one thing I would encourage you to think about.

---

93 *Abdelrazik v. Canada (Minister of Foreign Affairs)*, [2010] 1 FCR 267, 2009 FC 580

94 Canada, Parliament, Senate, Standing Committee on National Security and Defence,*Minutes of Proceedings and Evidence*, 41st Parl, 2nd Sess, (9 December 2013), testimony of Hon. Chuck Strahl, Chair of the Security Intelligence Review Committee, available online: http://www.parl.gc.ca/content/sen/committee/412%5CSECD/51109-E.HTM.

We note that SIRC's closest equivalent in Australia – the Inspector General of Security and Intelligence (IGSI)[95] – has jurisdiction not simply in relation to ASIO, the Australian equivalent to CSIS, but also the other members of the Australian intelligence community (although the IGSI's precise role varies from agency to agency). In this respect it is what in Canadian parlance one would call a "super SIRC" – that is, its remit extends between agencies and it not stovepiped to a single organization.

Elimination of the Inspector General

Up until recently, an inspector general also reviewed CSIS activity. This inspector general was appointed by the governor-in-council and was responsible to the deputy minister of public safety. Described as the minister's "eyes and ears" in the Service,[96] the inspector general monitored compliance by the Service with its operational policies and examines its operational activities.[97] To this end, the inspector general was given full access to the Service's information, except Cabinet confidences.[98] The inspector general also certified whether the reports provided by the director were adequate and whether they revealed any action of the Service that the inspector general views as an unauthorized, unreasonable or unnecessary exercise of its powers.[99] The Conservative government eliminated this position in 2012.

The move was unanticipated and, in fact, buried in the budget implementation bill. It was characterized as a cost-cutting measures, saving the government a very modest $1 million per annum. The government asserted that there would be no net degradation in review, because the inspector general's functions would be assumed by SIRC.

Commentators – including these authors – have critiqued the abolition of the inspector general as a net backwards leap in the CSIS accountability regime. The former Inspector General of CSIS was critical of SIRC's ability to take on the task of certifying CSIS's annual report to Parliament. It was reported by *The Canadian Press* in August 2012, that former Inspector General Eva Plunkett said it is "ridiculous" to think SIRC could do the same job of probing the Canadian Security Intelligence Service that her office did.[100]

---

95 Inspector-General of Intelligence and Security Act 1986, Act No. 101 of 1986, as amended,

96 Arar inquiry, Policy Report at 280.

97 CSIS Act, s. 30.

98 CSIS Act, s. 31. Cabinet confidences are, in essence, the papers supporting or describing Cabinet deliberations. For a definition of these papers, see *Canada Evidence Act*, s. 37; *Access to Information Act*, s. 69. For discussion, see Craig Forcese & Aaron Freeman, *The Laws of Government: The Legal Foundations of Canadian Democracy* (Toronto: Irwin Law, 2005) at 507 *et seq*.

99 CSIS Act, s. 33.

100 *The Canadian Press*, "Axing CSIS watchdog 'huge loss,' says former inspector general", (Aug 10, 2012), available online: http://www.cbc.ca/news/politics/axing-csis-watchdog-huge-loss-says-former-inspector-general-1.1143212.

She further commented that “they don't do the same kind of work at all,” and "they don't go into the same depth, the same detail. And they're basically part-time people.”[101]

The article states that “she noted that SIRC, while served by an executive director and staff, is composed of appointees who work part-time and meet in Ottawa only periodically. She suggested that's no substitute for taking on the task full-time, as she did, meeting with CSIS officials regularly at the agency's headquarters.”[102]

IG Plunket remarked that “It takes you at least a year in the job to learn the right questions to even ask the service,”and doubted that SIRC could fill the void left by her office without changing the way the Committee functions.[103]

SIRC added two additional staff members when it took on this new role. The inspector general’s office was staffed by 8 persons.

C. Need for Enhanced Review

We turn now to consideration of how to fix independent review in Canada

There is a widespread consensus among knowledgeable observers that that the present “stove-piped” or “siloed” nature of SIRC is inadequate. This consensus was most recently and most extraordinarily demonstrated just before the conclusion of 2nd reading of bill C-51 in the House of Commons when four former Prime Ministers, and former members of SIRC and former Privacy Commissioners released a joint letter. The letter made the case for enhanced self-initiated whole of government review and increased Parliamentary review of national security as something that was required both to protect rights and improve security. It also noted that the government had not implemented the review recommendations made by the Arar Commission in 2006.

Published in the Globe and Mail and LaPresse under the by-lines of Jean Chretien, Joe Clark, Paul Martin and John Turner, the letter has not made the impact we would have expected. It constitutes an important and extraordinary intervention and it deserves to be quoted in full:

> The four of us most certainly know the enormity of the responsibility of keeping Canada safe, something always front of mind for a prime minister. We have come together with 18 other Canadians who have served as Supreme Court of Canada justices, ministers of justice and of public safety, solicitors-general, members of the

101 *Ibid.*

102 *Ibid.*

103 *Ibid.*

Security and Intelligence Review Committee and commissioners responsible for overseeing the RCMP and upholding privacy laws.

Among us, we have served in our various public office roles from 1968 to 2014. Over that time we were faced with, and responded to, a range of pressing security concerns. We all agree that protecting public safety is one of government's most important functions and that Canada's national security agencies play a vital role in meeting that responsibility.

Yet we all also share the view that the lack of a robust and integrated accountability regime for Canada's national security agencies makes it difficult to meaningfully assess the efficacy and legality of Canada's national security activities. This poses serious problems for public safety and for human rights.

A detailed blueprint for the creation of an integrated review system was set out almost a decade ago by Justice Dennis O'Connor in his recommendations from the Maher Arar inquiry, which looked into the role that Canada's national security agencies played in the rendition and torture of a Canadian citizen. Justice O'Connor's recommendations, however, have not been implemented; nor have repeated calls from review bodies for expanded authority to conduct cross-agency reviews.

Meanwhile, efforts to enhance parliamentary oversight of national security agencies have also been unsuccessful. For example, in October 2004, a report calling for parliamentary oversight over national security activities was presented to the minister of public safety; this report contained an oversight structure that was agreed upon by representatives of all parties in both the House of Commons and the Senate. Legislation was introduced at the time, but not adopted before the next election.

Canada needs independent oversight and effective review mechanisms more than ever, 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.

Protecting human rights and protecting public safety are complementary objectives, but experience has shown

that serious human rights abuses can occur in the name of maintaining national security. Given the secrecy around national security activities, abuses can go undetected and without remedy. This results not only in devastating personal consequences for the individuals, but a profoundly negative impact on Canada's reputation as a rights-respecting nation.

A strong and robust accountability regime mitigates the risk of abuse, stops abuse when it is detected, and provides a mechanism for remedying abuses that have taken place. In the years since the Arar inquiry, international human rights experts – including the UN Committee against Torture – have called on Canada to improve oversight of its national security agencies.

Canada's national security policies and practices must be effective in order to protect public safety. Independent oversight and effective review mechanisms help ensure that resources devoted to national security activities are being utilized effectively and efficiently. The confidential nature of national security activities means that it is more difficult to rely on the usual public checks on government performance, such as scrutiny from Parliament, civil society, media and the general public. Security-cleared review bodies play crucial roles in catching and correcting operational and structural problems before they become full-blown national security failures leading to better security for Canadians.

National security agencies, like all government institutions, must be accountable to the public. Accountability engenders public confidence and trust in activities undertaken by the government, particularly where those activities might be cloaked in secrecy. Independent checks and balances ensure that national security activities are protecting the public, and not just the government in power. Oversight and review mechanisms are necessary to make sure that powers are being exercised lawfully, and that government officials are not called upon to undertake activities that might expose them or Canada to legal liability either at home or abroad.[104]

---

[104] "A close eye on security makes Canadians safer" Globe and Mail Feb 19, 2015. The letter was signed by: The Right Honourable Jean Chrétien, Prime Minister of Canada (1993-2003), Minister of Justice (1980-82); The Right Honourable Joe Clark, Prime Minister of Canada (1979-80), Minister of Justice (1988-89); The Right Honourable Paul Martin, Prime Minister of Canada (2003-06); The Right Honourable John Turner, Prime Minister of Canada (1984), Minister of Justice (1968-72); The

1. Reform Options

What then are the options for enhancing review in light of Bill C-51? We will focus here on independent review and address the question of parliamentary review later.

We note, first, the recommendations of the Arar Commission.

a) Getting Rid of Silos

The Arar Commission opposed silos. It recommended that "statutory gateways" be created between review agencies allowing them to cooperate closely, organized by a co-ordinating committee composed of the chairs of the three main review bodies (SIRC, CSEC Commissioner and RCMP reviewer) and an independent chair. Specifically, the Commission recommended "statutory gateways among the national security review bodies…in order to provide for the exchange of information, referral of investigations, conduct of joint investigations and co-ordination in the preparation of reports."[105] As Justice O'Connor explained in his report:

> It is essential that there be institutional co-operation among review bodies where there is institutional co-operation among the bodies being reviewed for four specific reasons: to avoid gaps in accountability, to attempt to avoid reaching inconsistent or differing conclusions about the co-operative activities; to provide a unified intake system for national security complaints, and to avoid the burden on agencies of duplicative review.[106]

Honourable Louise Arbour, Justice of the Supreme Court of Canada (1999-2004); The Honourable Michel Bastarache, Justice of the Supreme Court of Canada (1997-2008); The Honourable Ian Binnie, Justice of the Supreme Court of Canada (1998-2011); The Honourable Claire L'Heureux Dubé, Justice of the Supreme Court of Canada (1987-2002); The Honourable John Major, Justice of the Supreme Court of Canada (1992-2005); The Honourable Irwin Cotler, Minister of Justice (2003-06); The Honourable Marc Lalonde, Minister of Justice (1978-79); The Honourable Anne McLellan, Minister of Justice (1997-2002), Minister of Public Safety (2003-06); The Honourable Warren Allmand, Solicitor General of Canada (1972-76); The Honourable Jean-Jacques Blais, Solicitor General of Canada (1978-79); The Honourable Wayne Easter, Solicitor General of Canada (2002-03); The Honourable Lawrence MacAulay, Solicitor General of Canada (1998-2002); The Honourable Frances Lankin, Member, Security Intelligence Review Committee (2009-14); The Honourable Bob Rae, Member, Security Intelligence Review Committee (1998-2003); The Honourable Roy Romanow, Member, Security Intelligence Review Committee (2003-08); Chantal Bernier, Acting Privacy Commissioner of Canada (2013-2014); Shirley Heafey, Chairperson, Commission for Public Complaints against the RCMP (1997-2005); Jennifer Stoddart, Privacy Commissioner of Canada (2003-2013).

[105] Arar Commission, Policy Report at 606

[106] Ibid at 582

As all the facts we have marshaled in this backgrounder suggest, it is past incomprehensible why this change has not been made. This need not be a complicated legislative undertaking. Indeed, one of us has proposed simple legislative language that would accomplish much of this objective, reproduced in Annex 1.

ii) Expanded Review as Proposed by the Arar Commission

But whatever steps are taken to break down silos and to build statutory gateways, that will not alone be enough. Silos are one problem, but statutory gateways in many cases will be bridges to nowhere because of the absence of review for any bodies other than CSIS, CSE and RCMP.

The Arar Commission responded to this problem as well. Drawing on the facts of the Maher Arar case that involved CSIS, the RCMP, customs and Department of Foreign Affairs officials, it recommended that there should be independent review including self-initiated review and the hearing of complaints with respect to the national security activities of CBSA, Citizenship and Immigration Canada, Transport Canada, the FINTRC and Foreign Affairs and International Trade. A much better resourced SIRC would assume responsibility for the last four agencies and the RCMP review body would assume responsibility for the national security activities of the CBSA.[107]

Developments subsequent to the Arar Commission's 2006 report suggest that its list of agencies whose national security activities should be reviewed by SIRC is underinclusive. Both Bills C-44 and C-51 recognize and enable CSIS's expanding activities beyond Canada's shores. Leaving aside the merits of CSIS incrementally becoming a foreign as well a domestic intelligence agency, this expansion of CSIS's mandate suggests that SIRC's mandate should also be expanded to cover the intelligence functions of the Department of National Defence given the support role that CSIS has played for DND's operations both at home (ie. G20 summit in Toronto) and abroad (ie in Afghanistan and likely in Syria and Iraq).

More than this, the proposed s.22.3 of the CSIS Act in Bill C-51 contemplates that a judge may "order any person to provide assistance" that "may reasonably be required to give effect to a warrant" issued under ss.21 and 21.1. The judge may also order that the "person" offering assistance may be kept confidential in the public interest. Proposed s.24.1 also contemplates further assistance or subcontracting to "another person" provided certain proportionality based criteria are determined, presumably by CSIS itself. Such additional assistance would not be done by the authorizing judge but by a person in CSIS or potentially someone else included in the initial warrant.

One serious problem is that SIRC as presently constituted will not have clear jurisdiction to examine the activities of such other persons including those within

---

[107] Ibid Recommendation 9

government departments such as CSEC, Foreign Affairs and DND who are perhaps the most likely officials to be enlisted into help CSIS engaged in "kinetic" activities to reduce threats to the security of Canada.

We would stress, however, that the list is open-ended and could include private individuals or corporations or even foreign officials or governments. In order to fulfill its review functions properly and including the provision in bill C-51 that it "review at least one aspect of the Service's performance to reduce threats to the security of Canada"[108], SIRC should have jurisdiction and Inquiry Act powers to compel relevant information from anyone who has provided CSIS with assistance in executing its warrants.

Without such an expansion of its powers, there may be a possibility and even an incentive for CSIS to subcontract execution of its warrant to other parts of government or foreign governments or the private sector that are not subject to review.

Under s.24.1 this could be done even without the knowledge of an authorizing judge, in the event that we are even talking about the exercise of a power under warrant.

We are seriously troubled by the prospect of CSIS subcontracting disruption warrants to foreign agencies or officials. As we have said, since Canadian law rarely extends outside of Canada, CSIS would rarely reach the "trigger" point requiring it to seek a judicial warrant. Its overseas activities would mostly, therefore, be overseen by it alone and subject to limited audit-based review by SIRC.

Accountability for the conduct of foreign agencies or persons CSIS may enlist will be near impossible to guarantee. One of the lessons of the Maher Arar saga is that even the most robust of review bodies -- in that case a public inquiry with whole of government powers to compel the production of secret information -- is powerless in reviewing the actions of foreign government, even when an understanding of those actions may be essential to determining Canadian involvement in misconduct.

Unfortunately the broad subcontracting provisions of the CSIS Act are another example[109] of how bill C-51 demonstrates a striking disregard of the lessons of the Maher Arar inquiry.

iii) 'Super SIRC': Whole of Government National Security Review

A more ambitious alternative to the Arar Commission's recommendation would be to move to a "Super SIRC" model where one independent review body would be given sufficient powers and resources to review all of the government's national security activities. In other words, a strong case can be made that since the intensification of whole of government approaches to security since the 2006 Arar

---

[108] Proposed s.38 (1.1) of the CSIS Act in Bill C-51

[109] See our backgrounder #3 entitled "Sharing of Information and Lost Lessons from the Maher Arar Experience" Feb 16, 2015 at http://antiterrorlaw.ca

Commission report, including in the *Security of Canada Sharing of Information Act* in bill C-51 with its 17 designated recipient institutions, that the time has come to replace SIRC, the CSE commissioner and that part of the RCMP review agency that reviews its national security activities with one big committee or "super SIRC". The new committee should have jurisdiction to review all of the government's national security activities including security related information sharing.[110]

A "super SIRC" review body would have many advantages. It could follow the trail of intelligence, information sharing and other national security activities throughout government without the need for statutory gateways. It would provide a focal point for complaints about the government's national security activities. It would also eliminate concerns, recognized by the Arar Commission as legitimate, about duplicative review.

A one committee approach could also create possibilities for increased resources, full time members, broader representation of expertise and interests on the committee and increased staff with expertise dedicated to particular agencies.

We do not underestimate the demands or transition costs of creating a "super SIRC" or indeed even implementing the more limited expansion recommended by the Arar Commission. The existing core expertise of reviewing CSIS and reviewing CSE present in SIRC and the CSE Commissioner would have to be retained and integrated. Moreover, the new body would have to develop expertise working with a broad and diverse range of federal agencies including the RCMP, Foreign Affairs, DND, CBSA and so on.

We do not in this backgrounder purport to advance the full argument for such a body, or describe its parameters. That is a project for another day. Instead, we flag here the need for considerable thinking on this issue – thinking that should have pre-dated bill C-51 and which C-51 makes critical and urgent.

2. Comparative Developments in Review Reform

We end this discussion on reform of expert review in Canada with some data on comparative practice. We note that there is an emerging trend in our Five Eyes partners and elsewhere of whole of government review bodies.

Following recommendations from the 9/11 Commission, the US created a Privacy and Civil Liberties Oversight Board in 2004 intelligence reform legislation. This body has a whole of government remit and can offer advice on privacy and civil liberties on all terrorism policy issues, including information sharing. It considers

[110] This would greatly expand SIRC's mandate in part because of the breadth of the government's proposed security predicate for the Security of Canada Information Sharing Act. For criticism of this broad category of activities that undermine the security of Canada see Roach and Forcese "Backgrounder #3: Sharing of Information and Lost Lessons from the Maher Arar Experience" Feb 16, 2015 at http://antiterrorlaw.ca

reports from the privacy and civil liberties officers of 8 agencies including from the department of the Attorney General and Secretaries of Defence, State, Treasury, Health and Human Services, and Homeland Security and from the Director of National Intelligence and the Central Intelligence Agency. It also plays a co-ordinating role among the agencies.[111]

After one of its members resigned in 2007 claiming interference from the White House, the Board was re-constituted as an independent agency with five members including a full time chair serving staggering 6 year terms. The appointments to this Board must be ratified by the Senate. They are bi-partisan and have included retired public servants, judges and academics. One of its recent reports is impressive, examining both the NSA and FISA court performance in the collection of metadata.

The 200 page report was based on two public forums and on: classified briefings with officials from the Office of the Director for National Intelligence ("ODNI"), NSA, Department of Justice, Federal Bureau of Investigation ("FBI"), and Central Intelligence Agency ("CIA"). Board members also met with White House staff, a former presiding judge of the FISA court, academics, privacy and civil liberties advocates, technology and communications companies, and trade associations. The Board also received a demonstration of the USA PATRIOT Act's Section 215 program's operation and capabilities at the NSA. The Board has been provided access to classified opinions by the FISA court, various inspector general reports, and additional classified documents relating to the operation and effectiveness of the programs. At every step of the way, the Board has received the full cooperation of the intelligence agencies. Board staff have conducted a detailed analysis of applicable statutory authorities, the First and Fourth Amendments to the Constitution, and privacy and civil liberties policy issues. [112] This demonstrates impressive whole of government review work in a manner that engages the public.

In Australia, the Inspector General of Intelligence and Security has complaints and review jurisdiction over 6 different agencies spanning both civilian domestic and foreign intelligence agencies and military intelligence including signals intelligence and the office of national assessments. [113] As a result of 2010 legislation, the Australian IGIS can be tasked by the prime minister to inquire into any intelligence or security natter relating to any federal department or agency.[114] The Arar Commission in its examination of the Australian IGIS noted several advantages of its "multi-agency jurisdiction" including "a comprehensive view of the activities of various intelligence agencies" and the "ability to scrutinize integrated and

---

[111] 42 USC s.2000e.

[112] Privacy and Civil Liberties Oversight Board Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court, Jan 23, 2014 at 4, available at https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[113] Inspector General of Intelligence and Security Act, 1986 as amended

[114] National Security Legislation Amendment Act no 127 of 2010 sch 9.

information sharing activities." It also stressed that "a review body with such multi-agency jurisdiction must be properly resourced to fulfill its mandate."[115]

The UK has some whole of government security review. The Interception of Communications Commissioner reviews all intercepted communications regardless of what agency conducts the interception. Thus, the problems identified above of CSIS being assisted by other agencies in carrying out warrants and SIRC not being able to review the conduct of the assisting domestic agencies would not be a problem in the UK, at least as far as intercepts are concerned. Similarly the Office of Surveillance Commissioner reviews surveillance across multiple agencies.

It remains to be seen how the Privacy and Civil Liberties Board created under new British legislation will operate and how it will interface with the important work already done by the independent reviewer of terrorism legislation. But both of these bodies have wider remits than SIRC. And there is nothing apparent in this new legislation that limits the new Board to review of particular agencies.[116]

Legislation introduced in New Zealand in 2013 gave its Inspector General of Intelligence a wider remit to examine some system-wide issues and some issues with respect to signals intelligence and telecommunications, including hearing complaints from telecommunications companies. It also removed the requirement that the IG be a retired judge and provided for an advisory committee to assist with its work.[117]

B. Parliamentary Review

We have argued that expert review in Canada is very far from state of the art, is fractured, and is overwhelmed. The state of parliamentary review is unfortunately even worse.

1. Conventional Role of Parliamentary Committees

In many areas of government, parliamentary committees play a key role in holding ministers (and, *de facto*, their officials) to account. Parliament has powers to summon and even compel the appearance of officials,[118] including ministers.[119] Likewise, under the Common's Standing Orders, Standing Committees may "send for persons, papers

---

[115] Arar Commission, Policy Report at 326

[116] Counter Terrorism and Security Act, 2015 c. 6, ss.42-43.

[117] Office of the Inspector-General of Intelligence and Security Annual Report for year ending June 30, 2014 at http://www.igis.govt.nz/assets/ANNUAL-REPORT-2013-14.pdf

[118] See discussion in Derek Lee, *The Power of Parliamentary Houses to Send for Persons, Papers and Records* (Toronto: University of Toronto Press, 1999); *Telezone Inc. v. Canada (Attorney General),* (2004), 235 D.L.R. (4th) 719 at 726 (Ont. C.A.); *Canada (Attorney General) v. Prince Edward Island (Legislative Assembly)* (2003), 46 Admin. L.R. (3d) 171 (P.E.I. S.C.).

[119] Lee, *The Power of Parliamentary Houses* at 129 ("[u]nder the law, Ministers of the Crown enjoy no special status or privilege before the House or a committee").

and records."[120] Parliament and its committees may administer oaths requiring truthful responses,[121] a rarely utilized power. Parliament (and by extension, its committees) also posess contempt powers. Thus, "any act or omission that obstructs or impedes either House of Parliament in the performance of its functions, or that obstructs or impedes any Member or officer of such House in the discharge of his duty, or that has a tendency, directly or indirectly, to produce such results may be treated as contempt even though there is no precedent of the offence."[122]

All of this suggests that parliamentary committees are potentially potent review bodies in the area of national security. To date, however, parliamentary review in national security matters has not been robust. Both the senate and the House of Commons have national security and defence committees.[123] The senate defence and national security committees, in particular, have been active in holding hearings and producing reports on various aspects of Canada's national security and defence policy.

Parliamentary committees – and Parliament as a whole – have not, however, played a systemic or concentrated role in reviewing the activities of Canada's security agencies. Indeed, some critics describe their performance in this area as utterly inadequate.[124]

2. National Security Committee of Parliamentarians

The Canadian Parliament's record in national security matters compares unfavourably with that of other democracies. Most Western states have some sort parliamentary review, as described in a detailed 2011 EU report on the subject.[125]

Canada's system also compares unfavourably to other Westminster democracies. The United Kingdom, Australia and New Zealand have relatively potent national security parliamentary committees, bodies whose attributes are summarized in Table 2.

In 2004, the Canadian government tabled a discussion paper noting this comparative experience and identifying means of enhancing the parliamentary role in national

---

120 Commons *Standing Orders*, Order 108(1).

121 See *Parliament of Canada Act*, R.S.C. 1985 c. P-1, ss. 10–13.

122 Joseph Maingot, *Parliamentary Privilege in Canada* (Montreal: McGill-Queen's, 1997) at 193.

123 Standing Senate Committee on National Security and Defence; Special Senate Committee on the Anti-terrorism Act; House of Commons Standing Committee on Public Safety and National Security; House of Commons Standing Committee on Defence.

124 See, e.g., Douglas L. Bland & Roy Rempel, "A Vigilant Parliament: Building Competence for Effective Parliamentary Oversight of National Defence and the Canadian Armed Forces" (2004) 5 Institute for Research on Public Policy 1 [on-line].

125 Above note 3

security matters.[126] That more prominent role was endorsed in the subsequent national security policy, which proposed the creation of a "National Security Committee of Parliamentarians."[127] An interim committee of parliamentarians on national security also provided their views in October 2004, recommending a statutorily created committee of Parliament.[128]

Subsequently, in 2005, the then Martin government tabled Bill C-81 in the House of Commons to establish such a "National Security Committee of Parliamentarians."[129] The bill went no further than first reading in the Commons before it died on the order paper at the time of the 2006 election.

Had it been passed, the new law would have established something unusual in the Canadian context: a legislatively created committee comprising members from both the senate and Commons. The committee's members were to be appointed by the governor-in-council and to hold office during pleasure until the dissolution of Parliament. Given these terms, the committee was to be a *de facto* executive body, staffed by parliamentarians. Indeed, the bill explicitly specified that the committee was not a committee of Parliament and carved out exceptions to the general rules that parliamentarians cannot be employed by the executive branch. These provisions meant that the committee would enjoy none of Parliament's powers and privileges, including its inherent power to compel evidence and summon persons and hold persons in contempt. More than that, individual members' parliamentary privileges concerning immunity for the communication of information were emphatically abrogated.[130]

The committee was to have a broad mandate focused on reviewing

> (a) the legislative, regulatory, policy and administrative framework for national security in Canada, and activities of federal departments and agencies in relation to national security; and
>
> (b) any matter relating to national security that the Minister refers to the Committee.

---

126 Canada, A National Security Committee of Parliamentarians: A Consultation Paper to Help Inform the Creation of a Committee of Parliamentarians to Review National Security (2004) [online].

127 Government of Canada, Securing an Open Society: Canada's National Security Policy (2004) at 19.

128 Interim Committee of Parliamentarians on National Security, *Report* (October 2004) [online].

129 C-81, 1st Sess., 38th Parl., 53-54 Elizabeth II, 2004–2005.

130 Parliamentarians possess freedom of speech, meaning that a parliamentarian cannot be held liable for what is said in Parliament, at least on the floor of the House. *Re Ouellet* (1976), 67 D.L.R. (3d) 73 at 86 (Que. S. C.) (agreeing that "communications by a Member to another person outside the walls of the House are not covered by the privilege,") aff'd 72 D.L.R. (3d) 95 (Que. C.A.).

Committee members were to be sworn to secrecy and named "persons permanently bound by secrecy" under the *Security of Information Act*. The committee would be empowered to request information from ministers. The latter could provide any such information so long as compliant with the *Privacy Act*, not including Cabinet confidences. However, there was no requirement that the government supply the requested data, and information requests were to be judged by ministers with an eye to solicitor–client privilege, the extent to which the information concerned an actual investigation or operation, the provenance of the information from a foreign source, and the need to protect confidential sources and methods.

Reports prepared by the committee in the course of its functions were to be filed annually with the prime minister, who would then table a version in Parliament, redacted for information that would be injurious to national security, defence or international relations.

The bill and the committee proposal have not been resuscitated by the Harper government, although at one point it seemed likely that the current government would propose a system of parliamentary review of some sort.[131] In 2007, the Commons committee reviewing antiterrorism law recommended that the bill be re-introduced.[132] For its part, the special senate committee on antiterrorism law urged the creation of a standing senate committee to monitor, examine and report on national security law and policy on an ongoing basis.[133]

Table 2 Parliamentary Review in Commonwealth Countries

Attribute	Canada (as proposed in Bill C-81)	Australia	New Zealand	U.K.
Name	National Security Committee of Parliamentarians	Joint Committee on Intelligence and Security	Intelligence and Security Committee	Intelligence and Security Committee
Statutory basis	✔	✔ [134]	✔ [135]	✔ [136]
Bicameral representation	✔	✔	N/A	✔
Multiparty membership	✔ [137]	✔	✔	✔

131 Tonda McCharles, "Anti-Terror Measures Would Restore 'Preventive Arrests' and Help CSIS Spies Overseas," *Toronto Star* (16 May 2007).

132 House of Commons Subcommittee on the Review of the Anti-terrorism Act, *Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues* (March 2007) at 85 [on-line].

133 Special Senate Committee on the *Anti-terrorism Act*, *Fundamental Justice in Extraordinary Times* (February 2007)at 122.

134 *Intelligence Services Act*, Act No. 152 (2001), Part 4.

135 *Intelligence and Security Committee Act 1996*, 1996 No. 46.

136 *Justice and Security Act 2013*, c. 18, replacing Intelligence Services Act 1994, 1994, c. 13, s. 10

Review authority				
Administration and expenditures of security and intelligence agencies	✔	✔	✔	✔ [138]
Review any matter referred by minister	✔	✔	✔	
Review any matter referred by Parliament		✔		
Review operation and effectiveness of security law	✔	✔	✔	
Named operational areas excluded from review	✔ [139]	✔	✔	✔
Report directly to Parliament		✔	✔	✔
Report indirectly to Parliament through minister/Prime Minister	✔			
Rules on receipt and disclosure of secret information	✔	✔	✔	✔
Rules on secrecy obligations of members	✔	✔	✔	✔ [140]

3. More Recent Developments

Bill C-81 has since been resuscitated 5 times in subsequent Parliaments, as a Liberal private members bill. The most recent version -- sponsored by Wayne Easter -- is Bill C-551. This bill replicated the details of the Martin government project.

Meanwhile, Senator Hugh Segal recently introduced his own private members law project -- Bill S-220 -- in the Senate. This bill represents a stronger iteration of the Martin government law project, particularly on the absolutely key question of access to information. Bill S-220 denies committee members Cabinet confidences, but nothing else. Moreover, S-220 gives the committee power to compel the attendance of persons and papers. Bill C-551, in comparison, gives ministers the choice to supply information, and includes a long list of considerations ministers can take into account in declining to supply the committee with information.

A third private members bill – bill C-622 – sponsored by Liberal MP Joyce Murray was the most comprehensive reform project on offer in the present Parliament. For one thing, this bill sought to correct a key deficiency in Canada's oversight system:

---

[137] This aspect was not explicit in C-81, although clearly possible.

[138] Also includes reference to "operations", s.2, though not current operations.

[139] This exclusion was implicit. It was listed among the considerations that the minister was to take into account in deciding whether to provide information.

[140] Members of the committee are "notified" under the *Official Secrets Act, 1989*, 1987, c. 6, s. 1, and are therefore bound by that statute's strictures on security intelligence.

the lack of judicial oversight for CSE. On the parliamentary committee issue, the bill included important powers in terms of parliamentary committee access to information.

None of these private members projects has received government support.

4. Concerns about Overreach and Redundancy

In its present manifestation, the government has dismissed the virtues of a parliamentary committee. That rejection seems predicated on the belief that a parliamentary committee would engage in command and control oversight and that present systems of accountability are adequate.

We agree that parliamentary committees should not engage in real time oversight. Such activities are basically unknown in parliamentary democracies, as best as we can determine in preparing this backgrounder. We have suggested that there are better oversight reforms focused at the ministerial or agency head level or as suggested by the Air India Commission involving an enhanced oversight role for the PM's National Security Advisor.

Review, however, is a different matter, as we have repeatedly urged. In relation to claims about duplicative review (which the Arar Commission expressed concern about) or needless red tape, we note that the Australian parliamentary committee (a reasonably potent body) coexists in a system with an Inspector General. In other words, Australia has managed both expert and parliamentary review. It is unclear to us why Canada could not do the same.

Nor is there any merit to the view that a parliamentary committee would be "redundant" or "duplicative". For one thing, there is a critical need for "pinnacle" review. Even a super-SIRC would review a subset of national security activities with a focus on the propriety of actions. It would focus on more than its one, current "tree", but would still not be able to see the full national security "forest" and it will likely not focus on the efficacy or effectiveness of our national security systems.

In our system, no independent body sees the "forest". The Air India Commission stressed the dangers that the broader public interest might be lost in inevitable battles between security agencies with different and sometimes conflicting mandates. This is exactly the "forest like consideration" that might be contemplated in most other democracies by a specialized parliamentary review committee. A parliamentary committee is a supplement to expert committee review, not a replacement and not a competitor. We underscore again: this role as "pinnacle" reviewer is accomplished no where else in our system.

SIRC and other review bodies, or indeed a super SIRC, should be able to provide a security cleared parliamentary committee with its classified or unredacted reports. A cleared parliamentary committee should also be able to see unredacted Federal Court judgments in matters involving CSIS including with respects to its new powers and privileges under Bills C-44 and C-51. This would have the virtue of including

Parliamentarians within the ring of secrecy and in the feedback loop about the performance of security activities.

Parliamentarians should be concerned with both the propriety and efficacy of security activities. They could question the effects on both rights and security of CSIS conducting surveillance and "kinetic" activities in violation of foreign laws. The government has stressed (and exaggerated the extent to which) CSIS's new powers will be subject to judicial oversight, but judges are not in a position to make judgments about how CSIS's actions have affected Canada's foreign and economic relations with other countries. This is only one example where parliamentary review might contribute to a more careful assessment of unintended and perhaps harmful consequences arising from CSIS's new powers.

Another area that security cleared parliamentarians should monitor is the troubled relation between CSIS and law enforcement. As suggested above, the Air India Commission in its 2010 report raised serious concerns about how CSIS's focus on gathering intelligence might adversely affect terrorism prosecutions. CSIS now will have new statutory powers to give human sources privileges that will prevent them from being compelled to be witnesses for the prosecution or even to stop prosecutors from disclosing any identifying information about them, for example, when trying to sustain search warrants from Charter challenges. In the absence of enhanced executive oversight by the minister of public safety or, as the Air India Commission recommended, by the prime minister's National Security Advisor, a parliamentary committee with access to secret evidence should carefully evaluate relations between CSIS and law enforcement. The current threat environment makes it even more important to guard terrorism prosecutions as a viable means to incapacitate and denounce those who would use violence for political, ideological or religious objectives. Since as we have argued at length in backgrounder #2, bill C-51 creates substantial risk that prosecutions will become more difficult and protracted, earnest and regular review of this pattern is essential.

Past experience suggests that properly equipped, educated and with adequate good will, parliamentary review bodies can function well. They can contribute to a broader parliamentary and public competence where such competence is desperately required: enacting new national security law. We are regularly amazed at the relative degrees to which Westminster democracies manage national security law reform. We do not think that they always arrive at good outcomes, but the truth is that the UK Parliament is much more intelligently engaged on national security law issues than is our own.

We believe that this reflects the fact that Parliaments are given real responsibilities in this area, and often then try to live up to them. The contrast with our own recent parliamentary tradition is stark.[141]

---

[141] See Forcese, Craig, Fixing the Deficiencies of Parliament Review of Anti-Terrorism Law: Lessons from the United Kingdom and Australia (April 2, 2008). Choices, Vol. 14, No. 6, p. 2, May 2008. Available at SSRN: http://ssrn.com/abstract=1623472

The devil will always be in the details. A parliamentary committee, just like an expert review body, must be adequately staffed. Legislative committees in the US and the UK often have dedicated staff including legal counsel. This is not the norm for Canadian parliamentary committees. As should be apparent from all of our backgrounders, national security is an incredibly complex subject that involves many different departments and agencies and a wide variety of often complex laws. In addition, it is an area that should be informed by knowledge of comparative experience and human rights under both Canadian and international law. It will be very important that any parliamentary committee have staffing and resources that is adequate to the challenges of understanding and evaluating national security activities.

Conclusion

People are right to be concerned about whether CSIS's new powers in bill C-51 (and C-44) will be subject to adequate review and oversight. The government is wrong to suggest that all is well with accountability.

Clear thinking is required. Oversight refers to real time command and control strategies. Those who oversee security activities will be implicated in these decisions, and not then in a position to review them in an independent manner.

For exactly this reason, if no other, neither review bodies such as SIRC nor parliamentary committees are well-suited to perform oversight. In our system, responsible ministers perform oversight, to greater or lesser degrees. The minister of public safety has responsibility for both CSIS and, subject to police independence, the RCMP. The Air India Commission was not satisfied that this ministerial oversight was adequate, and proposed that the prime minister's National Security Advisor be given new powers to resolve disputes between CSIS's priorities in collecting intelligence and the RCMP's priority of law enforcement. The government has rejected this recommendation. There is, however, a need for a new oversight debate, especially about the effects that CSIS's new powers and privileges may have on terrorism prosecutions. The Air India Commission warned about the dangers of CSIS making decisions that favour their operational interest, but make subsequent terrorism prosecutions more difficult. Again, as per our discussion in backgrounder #2, we believe that bills C-51 and C-44 may turn out to be a legislated codification of this problem.

Although parliamentary committees are not suited to engage in operational real time command and control oversight, they can perform a valuable review function if they are adequately resourced and staff and able to have access to secret information. Canada alone of its 5 eyes partners does not allow any parliamentarian to have access to secret information. Indeed, it stands practically alone in the world's democracies in the degree to which it excludes parliamentarians from national security review functions.

This means that Parliament essentially flies blind on the details, and like the public is left wondering and uninformed about security failures such the October, 2014 attacks and our progress with interventions and investigations of suspected foreign

terrorist fighters. This must stop. The price for parliamentarian access to secrets is likely to be a statutory committee whose members are bound by secrecy laws and who cannot rely on parliamentary privileges.

Even more pressing in our view than the need for parliamentarians to have access to secret information is the need to reform SIRC to give it the powers and resources it needs to review CSIS's new powers. SIRC is a small body. Four members, an executive director, seventeen staff (of which three are lawyers) and an annual budget of less than $3 million to review CSIS with over 3000 employees and a budget over $500 million to engage in legally and operationally complex matters. As such SIRC can only audit an extremely small slice of CSIS's expanding activities. SIRC readily acknowledges that its reviews result "in a snapshot of the Service's actions in a specific case."[142]

The Arar Commission found in 2006 that review by SIRC was inadequate because it SIRC was stove-piped and could not go beyond SIRC. The situation has not changed, and has become more acute. In 2013, then Chair of SIRC stressed to a Senate Committee that while SIRC only had powers to review CSIS that "the trail is not going to stop nicely and neatly at CSIS's door." In words that are even more relevant today in light of Bill C 51 then they were in 2013, Mr. Strahl warned that SIRC will "come up to an imaginary wall" when it examines the conduct of other departments. He elaborated: "Other agencies, by necessity nowadays, are working closely with CSIS, and increasingly we're going to need some way of chasing those threads. Otherwise, we'll have to tell parliamentarians that, as far as we can tell, everything looks great in CSIS country, but we don't know what happened over that fence; you're on your own." [143] CSIS should work with other departments but SIRC should be able to examine how it works with other partners.

SIRC was a fenced-in body with inadequate legal powers to match whole of government security before Bill C-51: it will be even more inadequate after Bill C-51 becomes law.

Bills C-44 and 51 give CSIS more powers outside of Canada and bill C-51 contemplates that CSIS can have the assistance of "other persons" in carrying out activities, including some that may contravene Canadian law or the Charter. SIRC, however, will have no ability to review the actions of other federal departments, let alone "other persons" which may include foreign officials and entities.

The information sharing Act in bill C-51 will mean that CSIS can receive information from any other part of the government of Canada but that SIRC will be unable to follow the flow of information out. And there is no one else who could "get into the

---

[142] Security Intelligence Review Committee, *2011-2012 Annual Repor*t, p 6, available online: http://www.sirc-csars.gc.ca/pdfs/ar_2011-2012-eng.pdf at p 9.

[143] Canada, Parliament, Senate, Standing Committee on National Security and Defence, *Minutes of Proceedings and Evidence*, 41st Parl, 2nd Sess, (9 December 2013), testimony of Hon. Chuck Strahl, Chair of the Security Intelligence Review Committee, available online: http://www.parl.gc.ca/content/sen/committee/412%5CSECD/51109-E.HTM.

weeds." This new information sharing powers in bill C-51 come a year after a privacy commissioner report noted that its powers were inadequate in the national security context.

The new powers in bill C-51 are inherently flawed. As we have repeatedly said in our backgrounders, C-51 is so poorly constructed that it will provoke forseeable second order consequences that we earnestly believe will undermine our security.

But we also repeat our conclusion from backgrounders #2 and #3: More than anything, the increased CSIS powers and information sharing powers are irresponsible without a redoubled investment in our tattered accountability system. Anyone who has worked on accountability in the security sector knows that the core maxim is "trust but verify". We believe that current legal and resource constraints on review bodies mean that that standard cannot be met at present, let alone in relation to the proposed new powers.

Moving ahead with bill C-51 now, in its present guise, without a massive investment in accountability will mean that we will be trying to fix inevitable problems for years to come. Without a serious course correction, we risk serious accountability challenges in national security law, and the prospect of often avertible security scandals that simply diminish the credibility of the services and suck time and resources out of keeping us safe.

Annex I: Enhancing Coordination of Review Among Security Review Bodies to Reflect Recommendations of the Arar Commission

CSIS Act

56. (a) If on reasonable grounds it believes it necessary for the performance of any of its functions under this Act, those of the Commissioner of the Communications Security Establishment under the National Defence Act, or those of the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police under the RCMP Act, the Review Committee may convey any information which it itself is empowered to obtain and possess under this Act to:

> a) the Commissioner of Communications Security Establishment under the National Defence Act, or,
> b) the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police under the RCMP Act

(b) Before conveying any information referred to in paragraph (a), the Review Committee must notify the Director and give reasonable time for the Director to make submissions.

(c) In the event that the Director objects to the sharing of information under this section the Review Committee may decline to share the information if persuaded on reasonable grounds that the sharing of the information at issue under this section would seriously injure the Service's performance of its duties and functions under the Act.

(d) If the Review Committee dismisses the Director's objection, the Director may apply to a judge within 10 days for an order staying the information sharing.

(e) A judge may issue the stay order referred to in paragraph (d) if persuaded on reasonable grounds that the sharing of the information at issue under this section would seriously injure the Service's performance of its duties and functions under the Act.

(f) At any time, the Review Committee may apply to a judge for a lifting of any stay issued under paragraph (e) on the basis of changed circumstances.

(g) For greater certainty, the Review Committee may request information it believes necessary for the performance of any of its functions under this Act from the Commissioner of Communications Security Establishment under the National Defence Act, or, the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police under the RCMP Act.

National Defence Act

274.64 (a) If on reasonable grounds the Commissioner believes it necessary for the performance of any of the Commissioner's functions under this Act, those of the Security Intelligence Review Committee under the CSIS Act, or those of the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police under the RCMP Act, the Commissioner may convey any information which the Commissioner is empowered to obtain and possess under this Act to:

a) the Security Intelligence Review Committee under the CSIS Act, or,
b) the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police under the RCMP Act

(b) Before conveying any information referred to in paragraph (a), the Commissioner must notify the Chief and give reasonable time for the Chief to make submissions.

(c) In the event that the Chief objects to the sharing of information under this section the Commissioner may decline to share the information if persuaded on reasonable grounds that the sharing of the information at issue under this section would seriously injure the Establishment's performance of its duties and functions under the Act.

(d) If the Commissioner dismisses the Chief's objection, the Chief may apply within 10 days to a judge designated under section 2 of the CSIS Act for an order staying the information sharing.

(e) The judge may issue the stay order referred to in paragraph (d) if persuaded on reasonable grounds that the sharing of the information at issue in the application would seriously injure the Establishment's performance of its duties and functions under the Act.

(f) At any time, the Commissioner may apply to a judge for a lifting of any stay issued under paragraph (e) on the basis of changed circumstances.

(g) For greater certainty, the Commissioner may request information the Commissioner believes necessary for the performance of any of the Commissioner's functions under this Act from the Security Intelligence Review Committee under the CSIS Act, or the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police under the RCMP Act.

RCMP Act

45.471 (a) Notwithstanding any other provision in this Act, if on reasonable grounds the Commission believes it necessary for the performance of any of its functions under this Act, those of the Security Intelligence Review Committee under the CSIS Act, or those of the Commissioner of Communications Security Establishment under the National Defence Act, the Commission may convey any information which it itself is empowered to obtain and possess under this Act to:

a) the Commissioner of Communications Security Establishment under the National Defence Act, or,
b) the Security Intelligence Review Committee under the CSIS Act

(b) Before conveying any information referred to in paragraph (a), the Commission must notify the Commissioner and give reasonable time for the Commissioner to make submissions.

(c) In the event that the Commissioner objects to the sharing of information under this section the Commission may decline to share the information if persuaded on reasonable

grounds that the sharing of the information at issue in the application would seriously injure the Force's performance of its duties and functions under the Act.

(d) If the Commission dismisses the Commission's objection, the Commissioner may apply within 10 days to a judge designated under section 2 of the CSIS Act for an order staying the information sharing.

(e) The judge may issue the stay order referred to in paragraph (d) if persuaded on reasonable grounds that the sharing of the information at issue in the application would seriously injure the Force's performance of its duties and functions under the Act.

(f) At any time, the Commission may apply to a judge for a lifting of any stay issued under paragraph (e) on the basis of changed circumstances.

(g) For greater certainty, the Commission may request information it believes necessary for the performance of any of its functions under this Act from the Commissioner of Communications Security Establishment under the National Defence Act, or, the Security Intelligence Review Committee under the CSIS Act.