TSAS

canadian network for research on terrorism, security and society

Working Paper Series

No. 16-04

April 2016

Bridging the National Security Accountability Gap:

A Three-Part System to Modernize Canada's Inadequate Review of National Security

Craig Forcese and Kent Roach

The Canadian Network for Research on Terrorism, Security, and Society

TSAS is supported as a national strategic initiative funded by **SSHRC** and **Public Safety Canada**, along with the following departments of the federal government:

- Royal Canadian Mounted Police
- Canadian Security Intelligence Service
- Immigration, Refugees, and Citizenship Canada
- Correctional Services Canada
- Defence Research and Development Canada
- Global Affiars Canada
- Security Intelligence Review Committee
- Office of the Communications Security Establishmnet Commissioner

TSAS also receives financial support from several Canadian universities, including the University of British Columbia and the University of Waterloo.

 For more information, contact the Co-directors of the Centre, Daniel Hiebert, Department of Geography, UBC (daniel.hiebert@ubc.ca) and Lorne Dawson, Department of Sociology and Legal Studies, University of Waterloo (ldawson@uwaterloo.ca).

Table of Contents

Introduction 2

Part I: The Importance of Review 4

A. What is Review? 4
B. Why is Review so important? 5
C. What are the elements of effective review system? 6
1. Independence 6
2. Mandate 7
3. Bounded Transparency 8

Part II: What are Canada's Review Challenges? 11

A. What does it mean to say that Canada's review system is "stove-piped"? 12
B. What does it mean to say Canada's review system is "siloed"? 13
C. Propriety-centric Review 14

Part III: The Role of Parliamentarians 16

A. What role do parliamentarians presently have in review? 16
B. Is there a role in Canada for a Parliamentary Committee with Access to Secret Information? 19
1. Pinnacle Review and Review for Efficacy 19
2. Monitoring Trouble Spots 21
3. Ministerial References 21
4. Following Up on Classified Review Reports 22
5. Conducting Periodic Reviews of the Effects of Legislation 23
C. Are there risks in creating a committee of parliamentarians? 24
1. Lack of Trust 24
2. Perfunctory accountability and partisanship 25
3. Limited expertise and focus 26
4. Confliction with expert bodies 27
5. Review overload 27
D. What design would best achieve objectives and minimize risks? 28
1. Good people 28
2. Good Resources 29
3. Good Access to Information 30

Part IV: Fixing Expert Review in Canada: The Need for an S&I Community Reviewer 33

Part V: Independent Monitor of National Security Law 37

Conclusion 40

Bibliography 42

Appendix I: Annotated Legislation creating an Intelligence and Security Committee of Parliament 46

TSAS

canadian network for research on
terrorism, security and society

Working Paper Series

Bridging the National Security Accountability Gap: A Three-Part System to Modernize Canada's Inadequate Review of National Security

Craig Forcese

Faculty of Law, University of Ottawa

Kent Roach

Facutly of Law, University of Toronto

Abstract

We urge that Canada's reformed national security accountability review structure be built on the model of a three-legged stool: first, a properly resourced and empowered committee of parliamentarians with robust access to secret information, charged primarily with strategic issues, including an emphasis on "efficacy" review; second, a consolidated and enhanced expert review body—a "security and intelligence community reviewer" or "super SIRC"—with all-of-government jurisdiction, capable of raising efficacy issues but charged primarily with "propriety" review; and third, an independent monitor of national security law, built on the UK and Australian model, with robust access to secret information and charged with expert analysis of Canada's antiterrorism and national security legislation and able to work in concert with the other bodies on specific issues.

About this Project

We welcome (and very much encourage and need) feedback, critiques, suggestions and observations from other scholars, practitioners, security experts and interested persons with expertise to contribute (whether practical, legal, or scholarly). We thank those who have already provided valuable feedback and comments on an earlier draft. We are also grateful that twelve civil society groups have recommended the structure we propose in this paper as a starting point for consultations and as a "minimum" for national security accountability.[1]

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

1 See "Joint Open Letter on an integrated national security accountability framework" March 10, 2016, online: www.amnesty.ca/news/canada-bccla-joint-open-letter-integrated-national-security-accountability-framework

Introduction

Reasonable people in a democracy disagree over the appropriate balance between national security powers and rights. There should be much less disagreement about the need for adequate review of the state's national security activities.

At its core, the purpose of a national security system is: identification of national security threats; minimizing those threats; and (in performing these functions) acting in a manner that "preserves the country's ability to identify and to counter future threats with equal or greater effect."[2] Activities taken in pursuit of these objectives must be: lawful; proportionate to the threat; necessary in the context; and designed to be effective and efficient.[3]

"Review" must gauge security and intelligence (S&I) agency compliance with these standards,[4] in order to enhance effective oversight by ministers and officials of S&I agencies. While not all observers agree, we also believe that an important by-product of robust review is building public confidence in the integrity of the S&I community. Review is especially important because of the context in which S&I agencies operate. S&I agencies exercise substantial power, including the power to restrict rights and liberties and, if used excessively, violate those rights and liberties. S&I agencies must often exercise those powers in secret, and the efficacy and propriety of that conduct is not often or routinely subject to public scrutiny. S&I agencies insulated from this outside scrutiny and exposure may stray into patterns, policies, or groupthink impairing their effectiveness. Such practices may result in either overreactions causing human rights abuses or under-reactions causing security failures. S&I agencies are also publicly funded and, despite the secrecy around their conduct, should be accountable for their use of these monies.

While there is no clear reason to doubt the competency of the two review bodies that have, to date, performed national security review, Canada's present review structure does not provide sufficient safeguards. This was recognized in the 2006 report of the Arar Commission. It was confirmed by a February 2015 open letter signed by four former Prime Ministers and former high

2 Joe Fogarty, former UK security liaison to Canada, personal communication (December 2015; January 2016).
3 Ibid.
4 Ibid.

security officials. The weaknesses of the current safeguard regime have been acknowledged in regular comments made by existing review bodies about the challenges they face in performing their functions.

The previous government ignored this advice, but the new Liberal government has indicated a desire to improve the review of national security activities. The government has pledged to introduce a new parliamentary committee with access to secret information about national security.

This is a good first step that would allow Canada to catch up with most democracies. The merits of this body will lie, however, in how well it is designed. Moreover, its creation is not, alone, a sufficient step.

In this discussion paper, we urge that Canada's reformed review structure be built on the model of a three-legged stool:

- First, a committee of parliamentarians with robust access to secret (as in classified) information, charged primarily with strategic issues, including an emphasis on "efficacy" review—that is, focusing on the overall efficiency and effectiveness of Canada's S&I community, laws and policies. In designing this committee of parliamentarians, we must be attentive to three pivotal design aspects: good people; good resources; and good access to secret information.
- Second, a consolidated and enhanced expert review body—a S&I community-wide reviewer—with robust access to secret information, capable of raising efficacy issues but charged primarily with "propriety" review—that is, focusing on whether the S&I community is complying with law, policy and directives (including those dealing with rights and liberties), and also empowered to hear complaints concerning S&I community conduct;
- Third, an independent monitor of national security law, built on the UK and Australian model, with robust access to secret information and charged with expert analysis of Canada's antiterrorism and national security legislation and able to work in concert with the other review bodies.

Unlike Australia and the United Kingdom—jurisdictions that have (or will soon have) such three-legged review systems—Canada depends on a single leg: expert review. That single safe-

guard has failed to keep pace with the growth in collaborative and networked S&I activities since 9/11, including the many increased powers enacted in 2015. Canada's existing review structure is not fit for purpose: it is unduly constrained by fragmented and siloed jurisdictions, with essentially no independent review focused on the efficiency of the S&I system as a whole. This means that Canadians are at risk of security efforts that overreact and underreact to security threats.[5]

The precedents from Australia and the United Kingdom—as well as from the United States, where congressional committees and Inspectors General have access to secret information and which now has a Privacy and Civil Liberties Board—all suggest that a multi-pronged approach to review is necessary and will not be duplicative or excessive. Indeed, multi-pronged review reflects both the different purposes of review and the dynamic complexity and growth of S&I activities.

Review is a complex and imperfect system. All reviewers will only be able to review a small sample of national security activities. Matters can slip through the cracks. Review should be approached as a system with a certain amount of fail safes. Hence we propose in this paper a means to integrate the work of the three pillars of a renewed Canadian national security review system. We also suggest that the greatest possible transparency is necessary to ensure that review systems command public confidence. To this end, we propose a new system that will allow courts to decide unresolved disputes between reviewers and the government about what information can safely be placed in the public domain.

Part I: The Importance of Review

A. What is Review?

"Review" is the process by which independent bodies *retrospectively* evaluate the conduct of S&I agencies.[6] An effective review system is also prospective or forward-looking, and therefore able to evaluate the need for, and caliber of, proposed legislation or policy changes. A reviewer *does*

5 See generally Craig Forcese and Kent Roach *False Security* (Toronto: Irwin Law, 2015) Chap. 2 for discussion of Canada's history of over and under-reaction to security threats.

6 Many people call this process "oversight"–but in conventional Canadian practice "oversight" has traditionally meant operational control and coordination of security and intelligence services, something that is very different than "review". There is much misunderstanding, therefore, over who does or should do actual "oversight" in this classic sense. The general rule is: the executive. There is also a role for the courts to control S&I agency conduct through the warrant process. It is very important to understand that these

not have operational responsibility for what is being reviewed. The Security and Intelligence Review Committee (SIRC), the Communications Security Establishment Commissioner (OCSEC), and the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police (CRCC) are all examples of review bodies.[7] They review after the fact. They make findings and recommendations about the conduct that they review.

B. Why is Review so important?

There are five key reasons why review is important:[8]

1. S&I agencies exercise substantial power, including the power to restrict rights and liberties and, if used excessively, violate those rights and liberties. Given the nature of the threats they are designed to counter, they also have substantial discretion in deploying these powers. A bureaucracy immune to external scrutiny may find it difficult to resist the temptation to stretch uncertain boundaries.

2. Historically, S&I agencies (in Canada and elsewhere) have sometimes misused these powers. The entire architecture of the Canadian S&I community reflects a reaction to the abuses conducted by the RCMP Security Services in the 1970s. In the 2000s three separate and expensive commissions of inquiry had to be conducted into abuses and failures in the S&I community. Given the increased powers provided to security agencies in 2015, effective review is now more important than ever.

3. S&I agencies very often exercise their powers in secret. Those who have been investigated may be forever oblivious to this fact and in no position to complain about misconduct.

terms of "review" and "oversight" have different meanings in different places. When other countries talk about "oversight" they are often talking about what we in Canada would call "review". And when people talk about the US Congress having an "oversight" role, they refer to bundle of functions performed by Congress and congressional committees quite different from what happens in many other countries. The congressional role includes classic legislative activities, such as passing laws governing the S&I community and approving expenditures. Congressional committees also review, in the sense of probing past conduct. And the US executive also gives some congressional committees advance notification of certain sensitive covert foreign operations by US agencies, which leads some to regard Congress as performing a sort of supervisory function. In this paper, we are discussing "review" as the term is used in Canada, and not "oversight" either in the way that term is used in the United States or in the way that the term should be properly be used in Canada (that is, relating to operational command and control and coordination).

7 As we discuss further below, the RCMP CRCC has not yet commenced reviews in the national security context.

8 Summarized from Aiden Wills et al, Parliamentary Oversight of Security and Intelligence Agencies in the European Union (Brussels: European Parliament, 2011) ("European Parliament study"), online: issat.dcaf.ch/content/download/4148/36754/file/Parliamentary%20Oversight%20of%20Security%20and%20Intelligence%20Agencies%20in%20the%20European%20Union.pdf

Indeed, if no legal proceeding is commenced, no charge is laid and if 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.

4. S&I agencies are publicly funded and, despite the secrecy around their conduct, should be accountable for their use of these monies.

5. S&I agencies are generally insulated from the outside scrutiny and exposure that sometimes is essential to improve efficiency and effectiveness. S&I agencies may stray into patterns, policies, or groupthink impairing their effectiveness. Such practices may result in either over-reactions causing human rights abuses or under-reactions causing security failures. Review can counter this tendency. Moreover, review can contribute to an agency's legitimacy, especially where credible review findings counter misapprehensions about the S&I community in the media or public debates.

These considerations all point to the need for effective review mechanisms—audits and compliance systems able to measure agency compliance with legal and other standards of both propriety and efficacy, and query problematic behaviour. The appropriate relationship between democratic institutions and the security services in a democratic state must be: trust, but verify.

C. What are the elements of effective review system?

Different people categorize the elements of an effective review system differently. At minimum, an effective review system requires certain design elements:[9]

1. Independence

The review system must be independent of the government and the agencies that they review. The review bodies are not, in other words, both the watcher and the watched.

9 These themes represent a composite of those articulated by: Canada, 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, 2006) ("Arar Commission, Policy Report); Andrea Wright, "Casting a Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight and Review," Nicole LaViolette and Craig Forcese (eds) The Human Rights of Anti-Terrorism (Irwin Law, 2008); Ottawa Principles on Anti-terrorism and Human Rights (2006), Principle 9.3, online: http://aix1.uottawa.ca/~cforcese/hrat/principles.pdf

Independence obliges an appointment mechanism minimizing the perception that the appointee is beholden to the government or the S&I agencies. It also requires security of tenure, meaning that an appointee's job is not jeopardized if he or she curries disfavour within government or the S&I community because of the proper exercise of his or her functions.

Independence requires adequate resourcing and staff to meet the review body's mandate, and to develop and retain institutional knowledge.

Independence also means that the government should not have a unilateral veto over what information a reviewer should be able to disclose. Institutions will have competing interests in terms of disclosure, sometimes well-motivated and sometimes not. There should be provisions for independent resolution of disputes between reviewers and the government/agencies over what information should be publicly disclosed.

2. Mandate

Review bodies must be able to audit the *propriety* of security intelligence actions. Is the Canadian context, review assesses S&I agency conduct involving the Canadian Charter of Rights and Freedoms (the Charter), other law, ministerial directives, agency policy, international obligations and standards of propriety that are expected in Canadian society.[10]

A well-developed review system should also, however, include *efficacy* review. The public "whose security is at stake, whose tax dollars are being spent, and whose civil liberties and societal norms are in jeopardy … should have confidence that the system is functioning optimally to protect it."[11] Table 1 proposes key elements of both propriety and efficacy review, again emphasizing that in both instances the review body is performing a retrospective assessment and not engaged in advance authorization.[12]

10 Arar Commission, Policy Report 502.
11 Wright, *Casting a Light,* 336.
12 Wright, 334 et seq; Wills et al, *Parliamentary Oversight,* 104.

Table 1: Types of Review[13]

Type of Review	Qualities
Propriety Review	Monitors for compliance with law and policy and operational standards. Examines operational decision-making, and the manner in which the S&I agency secures compliance by its staff with these standards of propriety. Assesses criteria that the S&I agency uses to guide discretionary decision-making. Looks beyond conclusions and representations asserted by the S&I agency and audits the decision-making trail that leads to those conclusions and obliges S&I agencies to support decisions to deploy their powers. Includes reporting of non-compliance, an assessment of the reasons for non-compliance and recommendations for change. Because of the structure of governing laws, may be concerned with questions of proportionality in the exercise of S&I powers.
Efficacy Review	Evaluates strategic decision-making and operational competence, and the extent to which S&I agencies meet their objectives and meet the expectations of their stakeholders, including the government and the general public. Examines budget and resource allocation, recruitment, training and management and S&I agency policy formulation. Addresses questions of efficiency in terms of, e.g., resource allocation. Asks questions such as: Are government laws, rules, directives and policy objectives sound? Are the agencies being usefully deployed? Has the government deployed the intelligence it receives effectively?

3. Bounded Transparency

A viable review system requires three sorts of transparency.

Openness within the secrecy tent

First, the activities of the S&I community should be completely transparent to the review body itself—that is, it must possess powers to compel full access to information. More than this, "access depends on a good working relationships between the review agency and the service being scrutinized. It depends on the expertise and persistence of the review body staff. Struggles over access compound resource scarcities on the part of review bodies, leading to delays in reporting."[14]

Operating within this secrecy tent, review bodies wish their findings and recommendations to be read and followed by the S&I agencies, requiring a relationship of confidence between review body and agency. However, as Wark warns, too proximate a relationship "can distort the critical faculties and independence of a review body. It can also lead to an over-valuing of the relationship between reviewer and reviewed at the expense of the review body's public function."[15]

13 Wills et al, *Parliamentary Oversight*; Reg Whitaker and Stuart Farson, "Accountability in and for National Security," IRPP Choices 15, no.9 (2009): 39.

14 Wesley Wark, "Once More into the Breach: Strengthening Canadian Intelligence and Security Accountability," Canada2020 (March 2015). online: http://canada2020.ca/once-more-into-the-breach/.

15 Wark, *Once More into the Breach.*

Constrained but credible openness to the public

Second, the review bodies must themselves exercise transparency in relation to an external audience: the public. To this end, they must do more than simply provide "opaque assurances of propriety and effectiveness" to the public. Instead, review body assurances must be "informative, to the greatest extent possible without jeopardizing national security, providing information on the activities that are being undertaken, the policies that are being applies, the strategic priorities that are being pursued, the resources being expended, and the errors and deficiencies that are being identified and corrected".[16] Review bodies that are unable to demonstrate their value and ability to discover facts will not command public confidence.

Need to know considerations

However, both these forms of transparency are bounded by the necessity to control the distribution of sensitive information, especially operational information and information obtained in confidence from a foreign government. A review body is within the secrecy tent, giving it access to information necessary to perform its functions.

It is, as a consequence, subject to a "need to know" standard designed to ensure that information distribution is limited to those whose functions require access to the sensitive information, and no one else. The issues that likely raise the most acute concerns in relation to "need to know" are confidential source identity data and information provided by third party intelligence services. But "need to know" should be applied in a principled manner—not as reflexive culture of secrecy and not by ruling out categories of information to which the review body has no access. It should be guided by the same considerations of legality, necessity, effectiveness and efficiency that undergird the national security structure as a whole.[17] In a review context, need to know, therefore, is driven by the obligation to share information in a manner that contributes to the capacity of a review body to perform its functions—which include a wide-ranging consideration of efficacy and propriety, necessitating an expansive access to information.

Need to know presumably then applies within the review body itself, including one that

16 Wright, *Casting a Light*, 337.
17 Fogarty, personal communication.

has unrestricted statutory access to an agency's information. That statutory power does not then mean that *every* member of that review body should have access to the information, any more than every member of the S&I agency or community has access to the information.

A relationship of professional confidence between the review body of the S&I community obliges a review body to observe these standards in its own operations, and also to be careful in articulating its public findings in a manner that betrays no legitimately secret information. In this last regard, review bodies face an "on-going struggle to find ways to tell important national security stories in public without the deadweight of euphemistic language, the screen of obscurity, the excessive obeisance to official secrecy".[18]

Dispute settlement

The third form of transparency concerns, therefore, the manner in which disputes between a reviewer and a government will be resolved with respect to how much information can be made public. At present, parliamentary committees do not have such disputes simply because they do not have access to classified information. Review agencies such as SIRC do encounter these problems, but resolve them informally through negotiations with the government.

In our view, both parliamentary and expert reviewers could benefit from a more transparent process that allows for the independent adjudication of such disputes over secrecy. Such a process is not unprecedented and was used to resolve disputes between the Arar Commission and the government over how much information was made public by that commission.[19] The existence of such an option does not mean that solutions about what information reviewers can make public could no longer be negotiated. We expect that in most cases, a consensual resolution will occur. Nevertheless, in those few cases where agreement is not possible, there should be the option of adjudication in the Federal Court under s.38 of the *Canada Evidence Act*. This option should help to promote greater transparency and public confidence in the review process, especially in light of the conclusions drawn by both the Arar and Air India Commission that the government had over-claimed secrecy during the proceedings of those extraordinary, ad hoc review bodies.

18 Wark, 8.

19 *Canada (Commission of Inquiry) v, Canada (Attorney General)* 2007 FC 766.

Part II: What are Canada's Review Challenges?

Debate on Bill C-51 in 2015 often focused on whether its new powers would be subject to adequate review. Some of that debate focused on resourcing—SIRC in particular has been under resourced, but received increased funding in the April 2015 budget. By the time of this writing, that increased funding had yet to be realized, but was expected to be included in the government's supplementary estimates by mid-2016.

The more difficult questions were, however, legal and design ones. An increased budget for SIRC cannot compensate for the limits of its legal powers in reviewing the other federal agencies with which CSIS quite appropriately works in fulfilling its original and now expanded statutory mandate.

Based on Chatham House conversations involving security practitioners, watchdogs and academics (2015 Canadian Association of Security and Intelligence Studies (CASIS) Roundtable), there is broad (though certainly not universal) agreement that the current accountability system—of which review is a pivotal component—fails to meet public expectations, does not build trust and compares unfavourably to that of our close intelligence allies.[20]

In February 2015, four former prime ministers—Jean Chrétien, Joe Clark, Paul Martin and John Turner—published open letters in *La Presse* and the *Globe and Mail*. They argued "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."

The former Prime Ministers, joined by former members of SIRC, Privacy Commissioners, and former judges, noted the government had not implemented either the 2006 recommendations of the Arar Commission for expanded independent review or earlier Martin government proposals that would have given a statutory committee of parliamentarians access to secret information. They concluded that the new powers in bill C-51 meant "Canada needs independent

20 CASIS, *Roundtable Discussion of Accountability of Security and Intelligence Agencies*, Ottawa, June 4, 2015

oversight and effective review mechanisms more than ever".[21] In its study of Bill C-51, the senate national security committee recommended that the "government should develop statutory authorities among the national security bodies, in order to provide for the exchange of operational information, referral of investigations, conduct of joint investigations and coordination in the preparation of reports."[22]

The fundamental problems identified by the Arar commission of inquiry a decade ago remain. Specifically, the existing review bodies are legally "stove-piped" and "siloed". Canadian review is also mostly confined to propriety and does not include any real efficacy review.

A. What does it mean to say that Canada's review system is "stove-piped"?

Canada's persists in an unfortunate pattern of limiting independent, expert review to only three security agencies: SIRC for CSIS, OCSEC for the CSE, and (to a lesser degree) the CRCC for the RCMP.

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 new *Security of Canada Information Sharing Act*,[23] which allows most federal institutions to share security information with seventeen different departments. Again, only three of these bodies (CSIS, CSE, and the RCMP) are subject to national security review.

The Canada Border Services Agency (CBSA) presents a particularly obvious omission. CBSA

21 "A close eye on security makes Canadians safer" *Globe and Mail* (19 Feb 2015), online: http://www.theglobeandmail.com/globe-debate/a-close-eye-on-security-makes-canadians-safer/article23069152/. 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 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).

22 Standing Senate and Defence Committee, Reports and Observations on C-51 (May 27, 2015), online: http://www.parl.gc.ca/Content/SEN/Committee/412/secd/press/27may15-e.htm.

23 SC 2015, c 20, s 2.

performs both law enforcement and intelligence functions. It also shares information with other agencies, including CSIS. It is subject to no independent review, an omission that has attracted regular recommendations for change.[24] 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.

There are a few agencies with very narrow and specific mandates that perform all-of-government review, such as the Privacy Commissioner (for privacy) and the Auditor General (for financial management). But these last two bodies have neither the mandate nor the expertise to review national security operations per se. Indeed, in a report released in early 2014, the Office of the Privacy Commissioner commented adversely on its power to review national security information sharing powers, despite their significant impact on privacy. [25]

B. What does it mean to say Canada's review system is "siloed"?

The existing review bodies are unable to work collaboratively with each other, even as the agencies they review do precisely that. That is, review bodies are confined to their "silos".

The CSIS review body, SIRC, still lacks statutory authority to examine the large number of other federal agencies with which CSIS increasingly and sensibly works, despite the 2006 Arar Commission recommendations that would have allowed it to conduct joint investigations and exchange information with the OCSEC (when CSIS works with CSE) and with the CRCC (when CSIS works with the RCMP).

As a result, SIRC, OCSEC and CRCC are able to review only part of the Canadian government's national security apparatus, even while it is the public interest and an accelerating practice that S&I agencies work collaboratively. And when the existing review bodies do review the narrow subset of bodies, they cannot collaborate in sharing secret information or conducting joint review investigations. Moreover, like SIRC and other reviewers, the Privacy Commissioner's office lacks the power to conduct joint investigations with other review agencies, even while

24 See, e.g., Standing Senate and Defence Committee, *Vigilance, Accountability and Security at Canada's Borders* (June 2015) at Recommendations 1 and 2, online: http://www.parl.gc.ca/Content/SEN/Committee/412/secd/rep/rep16jun15a-e.pdf.

25 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*, 2014.

the agencies it is reviewing are increasingly conducting joint operations. In other words, it too is kept to its silo.

As a result, review bodies complain they cannot "follow the thread" between agencies conducting joint operations. That means reviews of S&I community conduct are, at best, approximate. SIRC has warned on several occasions that it has only been able to conduct partial reviews and was unable to follow the CSIS trail when it led to the Canadian Forces, CSE or other agencies.[26]

C. Propriety-centric Review

Finally, the Canadian system of review is almost entirely propriety (and not efficacy) review. The existing expert review bodies are compliance-oriented entities, gauging S&I agency conduct against standards of propriety.[27] There is little efficacy review in the Canadian system, except in so far as the Auditor General occasionally examines one or more members of the S&I community on a subject matter specific issue (such as information-sharing).[28]

The myopic focus on propriety review is unfortunate. As Farson and Whitaker note (rightly) "[i]n recent years, some of the most crucial questions that have required external independent review have been precisely those of efficacy arising out of catastrophic intelligence failures."[29] A thorough examination of the Air India matter constitutes one example—and it was delayed by decades because efficacy review depended on the ultimate political decision to appoint an ad hoc commission of inquiry. There has yet to be a thorough and independent review of the terrorist attacks of October 2014.

---

26 See discussion and enumeration of these warnings in Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism* (Irwin Law, 2015), Chap. 12.

27 This singular focus is strongest in relation to OCSEC, a body whose review function is confined to examining "compliance with the law". NDA, s.273.63(2). The RCMP CCRC has yet to perform a review function – a mandate that is, at any rate, subordinated to its principal function as a complaints body. At any rate, its governing law steers it exclusively to propriety review: it is to review "the activities of the Force are carried out in accordance with this [RCMP] Act or the *Witness Protection Program Act*, any regulations or ministerial directions made under them or any policy, procedure or guideline relating to the operation of the Force". RCMP Act, s. 45.34(1). SIRC's remit is, in principle, broader and reaches reviewing "generally the performance by the [Canadian Security Intelligence Service of its duties and functions". CSIS Act, s.38. Whether by tradition or reason of resource constraints, our sense for SIRC's public reports is that its reviews amount essentially to propriety review.

28 See 2009 March Status Report of the Auditor General of Canada, online: http://www.oag-bvg.gc.ca/internet/English/parl_oag-_200903_01_e_32288.html#hd3a

29 Farson and Whitaker, *Accountability in and for National Security*, 35.

Moreover, the rapid change in technology and a changing threat environment has rendered many Canadian laws inadequate to their original purpose. There is no review body that evaluates regularly whether existing laws are adequate.

Propriety review will never be able to challenge, for instance, a measure that complies fully with a law, but that is ineffective in addressing a security threat. A review of CSIS for propriety may, for instance, determine whether that agency is following the letter of the law in exercising its new, post-C-51 threat reduction powers. Propriety review does not, however, focus on whether that lawful conduct makes sense from a strategic perspective or whether, instead, it has negative knock-on effects in relation to other security objectives, such as making it more difficult to prosecute terrorists. This as a significant omission since we predict that uncritical deployment of new C-51 powers will have such negative knock-on effects.[30]

Similarly, efficacy-based review is important with respect to the signals intelligence work of the CSE. A key unexamined question is, for instance, to what extent does the collection and manipulation of "big data" actually produce actionable intelligence?

Further, an almost exclusive focus on propriety review—coupled with the stove-piping phenomena—means that "greater attention has been paid to the collectors of intelligence – those on the sharp end of the process, with the capacity to intrude on civil society and intimate and coerce. …[S]everal elements of the intelligence community that do not participate in intelligence collection…are not routinely considered."[31] Review for efficacy would oblige a more holistic focus on all agencies work together (or not) in responding to security threats.

It is important to underscore, however, that efficacy and propriety are sometimes interconnected. For example, it is not always possible or sensible to ignore efficacy-based considerations when determining whether limits on rights are reasonable and proportionate. Likewise, propriety findings may inform conclusions on efficacy issues. For instance, conduct may be efficacious, but illegitimate and illegal. Therefore, review should be concerned with both the propriety and the efficacy of the government's security efforts and the review system as a whole should avoid

30 See Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism* (Irwin Law, 2015), Chap. 9.
31 Farson and Whitaker, *Accountability in and for National Security*, 38.

new, artificial barriers stove-piping efficacy and propriety review. The best image may be that of a Venn diagram, in which efficacy and propriety issues occupy their own domain, with the prospect of overlap between them.

Part III: The Role of Parliamentarians

A. What role do parliamentarians presently have in review?

Canada is alone among its "Five Eyes" partners (the United States, the United Kingdom, Australia, and New Zealand) in not giving any parliamentarians (other than ministers) routine access to secret information. Indeed, as portrayed in table 2 below, it is close to alone among Western democracies in this respect.[32] The weight of opinion at the 2015 CASIS Roundtable was that "the absence of a formal parliamentary review mechanism was an anomaly and that parliamentary review needed to be part of any system intended to build public confidence and trust".

Table 2: Parliamentary Access to Secret Information[33]

	Countries for which data are available
Countries that deny parliamentarians access to secret information	Canada, Ireland
Countries that permit at least some parliamentarians access to secret information	Australia, Austria, Belgium (limited to lowest classification level), Bulgaria, Czech Republic, Denmark (but not "top secret"), Estonia, Finland, France, Germany, Hungary, Italy, Lithuania, Netherlands, New Zealand, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, United Kingdom, United States

Former senator Hugh Segal argues (correctly) that Canada's peculiar reluctance to give its parliamentarians a meaningful role in national security is unacceptable because it "means that elected Canadian legislators, unless ministers, are essentially out of the loop, lacking and having no way to acquire the expertise and facility necessary to conduct competent, diligent and discrete legislative oversight on behalf of Canadian taxpayers."[34] A 2004 Martin government discussion

32 See Nicholas MacDonald, "Parliamentarians and National Security in Canada" (2011) *Canadian Parliamentary Review* 33; Wills et al, *Parliamentary Oversight.*

33 Data drawn from Wills et al, *Parliamentary Oversight*, 119 and Craig Forcese, *National Security Law* (Irwin Law, 2007): 113.

34 Hugh Segal, "Freedom and Security: The Gordian Knot for Democracies" in *After the Paris Attacks: Responses in Canada, Europe and around the Globe*, ed. Edward Iacobucci and Stephen Toope. (Toronto: University of Toronto Press, 2015): 177.

paper noted "the current structure of [parliamentary] committees provides a limited basis for substantive parliamentary engagement on national security matters".[35]

In short, parliamentarians on Senate and Commons standing committees have been denied the full and wide-ranging access to secret information that is needed to ask the right questions of security officials in any expectation of meaningful answers. They have been unable (and in many cases unwilling) to resist the notorious reluctance of security officials to volunteer information. In a recent example, the Senate standing security committee wrote, with understated frustration, about the challenges associated with its study on Canadian security risks: "the committee was concerned by its inability to extract a direct answer from officials about the number of Canadians that have left to join terrorist groups abroad."[36]

This situation persists, despite quasi-regular and cross-party calls for reform over the last 35 years. For example:

- In 1981, the McDonald Commission examining wrongdoing by the RCMP Security Service—CSIS's predecessor—recommended the creation of a joint parliamentary committee on intelligence, able to hear classified information in private. The commission recognized the risks of leaks, but concluded that Canadian legislators were no less trustworthy than those in other democracies.[37] The government of the day rejected this recommendation.
- In 2004, the Martin government tabled a discussion paper looking to the foreign experience and identifying means of enhancing the parliamentary role in national security matters.[38] It

35 Government of Canada, *A National Security Committee of Parliamentarians: A Consultation Paper to Help Inform the Creation of a Committee of Parliamentarians to Review National Security* (Ottawa, 2004) (Martin discussion paper): 13. online: http://www.collectionscanada.gc.ca/webarchives/20060203031639/http://ww2.psepc-sppcc.gc.ca/publications/national_security/nat_sec_cmte_e.asp. To be sure, some regular parliamentary committees—especially in the unelected Senate—have issued some valuable reports revealing deficiencies in Canada's security operations. And in 2010, parliamentarians in a minority Parliament asserted their ancient parliamentary privileges in an attempt to hold government to account by compelling access to secret documents in the Afghan detainee controversy. For a discussion of the affair, see Heather MacIvor, "The Speaker's Ruling on Afghan Detainee Documents: The Last Hurrah for Parliamentary Privilege?" (2010) Constitutional Forum, 19: 129. But that protracted effort to examine whether the Canadian military was complicit with torture when it transferred Taliban detainees in Afghanistan to Afghan officials resulted in no lasting reforms. Instead, it produced an ad hoc compromise with government that allowed a few members of Parliament, assisted by retired judges, to have limited access to at least some secret documents. This $12-million process culminated in the disclosure in redacted form of a minority of the requested documents. But the matter eventually lost political momentum, and the work of the ad hoc committee did not continue after the majority Conservative government was elected in 2011.

36 Senate Standing Committee on National Security and Defence, *Countering the Terrorist Threat in Canada: An Interim Report* (July 2015): 10. online: www.parl.gc.ca/Content/SEN/Committee/412/secd/rep/rep18jul15-e.pdf [Countering the Terrorist Threat].

37 Commission of Inquiry Concerning Certain Activities of the RCMP, *Freedom and Security under the Law* (Ottawa: Supply and Services Canada, 1981): 902.

38 Martin discussion paper. See also Government of Canada, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Privy Council Office, 2004): 19.

proposed the legislative creation of a "National Security Committee of Parliamentarians" in its 2004 security policy. An interim committee of parliamentarians recommended a committee with access to secret information modeled on that possessed by SIRC, and with members who were sworn to secrecy but otherwise clothed in parliamentary privilege.[39] In 2005, the Martin government tabled Bill C-81 to establish such a "National Security Committee of Parliamentarians."[40] The bill went no further than first reading in the Commons before it died on the order paper with the dissolution of Parliament for the 2006 election. Bill C-81 has been resuscitated five times in subsequent Parliaments, generally as a Liberal private member's bill. It has never passed. The most recent version—sponsored by former solicitor-general Wayne Easter—replicated the details of Bill C-81, but failed to reflect the 2013 upgrade to the powers of the United Kingdom committee that had inspired the original Martin-era proposal.[41]

- Conservative Senator Hugh Segal proposed a stronger bill in the most recent Parliament, based on 2011 recommendations by a Senate special committee reviewing anti-terrorism law. The Segal bill followed the SIRC model of giving members access to everything except cabinet confidences.[42] It also proposed giving the committee the traditional powers of parliamentary committees to compel the attendance of persons and the production of papers.[43]
- Liberal MP Joyce Murray sponsored a third private member's bill, which was also on the parliamentary roster in the last Parliament.[44] It built on Senator Segal's proposed "Intelligence and Security Committee of Parliament" with six members of Parliament and three senators. Unlike earlier proposals, it attempted to counter majority-party domination by providing that no more than four members could be from one political party. The committee could also retain its own staff—an important feature of any committee wishing to become an independent source of expertise. Following the SIRC model and like its counterpart in the Segal bill, the committee would have access to all information except cabinet confidences, and its members would be permanently bound to secrecy under the strict terms of the *Security of Information Act*.

39 Report of the *Interim Committee of Parliamentarians on National Security* (October 2004). online: www.pco-bcp.gc.ca/docs/information/publications/aarchives/cpns-cpsn/cpns-cpsn-eng.pdf.

40 Bill C-81, *An Act to establish the National Security Committee of Parliamentarians*, 1st Sess, 38th Parl, 2004–2005.

41 Bill C-551, *An Act to establish the national security committee of Parliamentarians*, 41st Parl, 2d Sess, 2013. In the UK, the ISC obtained greater independence from the executive and greater access to information, although whether these changes will resolve some of the concerns about the ISC model discussed below remains to be seen.

42 Cabinet confidences are, in essence, the papers supporting or describing cabinet deliberations. For a definition of these papers, see *Canada Evidence Act*, RSC 1985, c C-5, s 37; *Access to Information Act*, RSC 1985, c A-1, s 69.

43 Bill S-220, An *Act to establish the intelligence and security committee of Parliament,* 41st Parl, 2d Sess, 2014.

44 Bill C-622, CSEC *Accountability and Transparency Act,* 41st Parl, 2d Sess, 2014. In the interest of transparency, one of us was consulted on the drafting of this bill but takes no credit for its content.

None of these law proposals went any further than first reading in the prior Parliament.

As a result, nothing has changed in the area of national security legislative accountability since the rejection of the McDonald Commission's recommendations 35 years ago.

B. Is there a role in Canada for a Parliamentary Committee with Access to Secret Information?

We think there is value in a National Security Committee of Parliamentarians—that is, a special, statutorily created administrative entity whose members are parliamentarians. This body is necessary because Canada has no review entity currently focused on "systemic" issues or with a "whole of government" mandate to match the government executive's whole of government approach to security and because of the lack of efficacy-based review under Canada's inadequate review system. For these reasons, we believe it is patently incorrect to claim that a Committee of Parliamentarians (CoP) would constitute redundant "red tape", a speaking point deployed regularly by the last government during debates over C-51.

Laying out our argument in fuller form, we favour a Canadian Committee of Parliamentarians (CoP) for the following reasons:

1. Pinnacle Review and Review for Efficacy

An European Union (EU) Parliament report concludes, rightly in our view, that what matters is that some independent accountability body *somewhere* is in a position to scrutinize policies, administration and financing, past operations and ongoing operations.[45] That is, some review body or set of review bodies should assess the S&I community on both propriety and efficacy grounds. There must, in other words, be complete coverage.

A CoP with access to secret information would be in an excellent position to see and evaluate the full national security "forest" while expert review bodies probe the minutiae. And parlia-

45 Review of ongoing operations raises the greatest conundrum, since confidentiality concerns will be most acute here. We would not support review morphing in oversight, in the form of approval of operations in large part because of concerns that this might undermine the independence and effectiveness of the review function. But we do think that aspects of ongoing operations can be subject to review. For instance, a warrant obtained in the course of the operation should plausibly be subject to review, even if the investigation as a whole is not completed. A bright line rule against reviewing all ongoing operations (which may be quite attenuated) might shield too much agency conduct from review. This development would be especially troubling where the shielded operations involve the exercise of novel and/or intrusive powers.

mentarians with a broad democratic remit and charged with a distinctive public policy function in our system are more plausibly positioned to examine efficacy issues than are the expert review bodies. The executive inevitably has a vested interest in defending its own actions and parliamentarians can bring fresh eyes and be more representative of the Canadian public. A CoP could, therefore, become the specialist in all-of-government "big picture" efficacy review and in asking challenging questions about executive conduct in the national security field. The 2004 Martin discussion paper contemplated that "the over-arching purpose of parliamentary review is to improve the effectiveness of our security arrangements by making them more accountable through the central organ of our democracy, the Parliament of Canada."[46]

The division of labour between CoP and expert review bodies follows from this CoP strategic mandate. Generally speaking, we think it wise to focus expert review bodies on a mostly propriety-based role rather than have them take on a full-fledged efficacy review responsibility as well. Assigning the same body both a propriety and efficacy mandate "could immerse the body at times in results-based examinations of matters such as the choices of investigative methods and selection of targets, and even budgetary considerations". This could "consume valuable resources and skills, and would effectively involve the body in strategic decision-making," possibly diverting "the body from its priority mandate of reviewing activity for propriety, and taint it objectivity."[47]

European experience suggests that a parliamentary body could embark on propriety review, if adequately designed. This risks, however, diluting the efficacy focus, and also creating conflict with the expert review system. Moreover, it is worth noting that at least some of the critique aimed at the UK Intelligence and Security Committee (ISC) seems provoked by that committee's lacklustre interventions in the area of propriety review.[48] For example, the UK government found it was necessary to appoint a public inquiry to examine the propriety-based issue of possible complicity in torture.

46 Martin discussion paper, 24.
47 Wright, *Casting a Light,* 356.
48 See Ian Leigh, "Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11, Intelligence and National Security, (2012) *Intelligence and National Security*, 27 no. 5: 722-727.

We add a word of caution: it is logical to create a division of labour between propriety-oriented, expert review bodies and an efficacy-oriented CoP, combined with information-sharing protocols permitting these separate review bodies to share information. It would be illogical, however, to create watertight compartments segregating propriety and efficacy review. If the CoP is primarily an efficacy-review body, it should nevertheless be able to examine propriety issues that relates to its more strategic concerns. Likewise, expert review bodies should be competent to raise efficacy matters stemming from their propriety reviews.

2. Monitoring Trouble Spots

Parliamentarians with access to secret information could monitor trouble spots that emerge among security agencies.

For instance, in our present system, no review body is positioned to comment on whether there is satisfactory whole-of-government co-ordination and information sharing. Indeed, a CoP with access to secret information might have been able to conduct a lessons learned exercise about the October 2014 terrorist attacks; something that has yet to be done by an independent body and might otherwise be difficult in Canada without the appointment of a commission of inquiry, like the Arar Commission, the Air India Commission and the Iacobucci Commission. Indeed, such a study might well be an appropriate starting task for any new CoP.

3. Ministerial References

We also think it is important that ministers with national security responsibilities or the prime minister be able to task a new CoP with specific investigations, a function to date performed by ad hoc commissions of inquiry.

Although commissions of inquiry have made important contributions to the development of Canadian national security policy, they cost a fortune, take much time, and can themselves be delayed by legal challenges. In some cases, a well-researched CoP inquiry and report could be more timely and certainly less expensive.

Moreover, recommendations made by a CoP may have a better chance of being implement-

ed than those made by commissions of inquiry, which dissolve at the end of their activities and can conduct no follow-up.

4. Following Up on Classified Review Reports

A CoP with access to secret information would be competent to review the many confidential reports that SIRC and OCSEC routinely provide to ministers. Holding hearings as a follow up to expert review body reports appears to be common in those European jurisdictions with both expert and parliamentary review bodies.[49]

A CoP with full access to those reports would be in a position to scrutinize both how well expert review bodies are performing their (primarily) propriety review function, and also how well ministers are performing their executive oversight function in response to review findings. No one is currently in a position to assess either of these forms of accountability in Canada.

Such follow-up is especially important, given that reviewers can only make findings and recommendations. Specifically, the CoP could question ministers on how they responded to the classified findings and recommendations from expert watchdog reviewers. And a CoP could, in appropriate circumstances, question a minister in public about a failure to address expert body recommendations, without revealing any of the secret details. Such questioning could improve the critical process of ministerial oversight of agencies. It could also attempt to break down silos by questioning multiple ministers about how different agencies work together (or not) on important cross-cutting security matters.

Participants in the 2015 CASIS Roundtable contemplated a model of CoP that would be empowered to task existing expert review bodies to perform investigations. A CoP able ask the expert review body to conduct follow ups, either in relation to its own investigations or on matters that the CoP encounters in its own work, allows handover between expert and CoP reviewers, ensuring that Canada does not labour under a new form of siloed review. That said, a CoP should be cautious not to overburden another review agency in a way that detracts from the tasked review agency's mission or independence. Reviewers are the best judges of how to devote

49 Wills et al, *Parliamentary Oversight*, 109.

their limited resources to an inevitably partial audit of security activities. In general, the reviewer to whom such an undertaking is delegated should have some discretion to decline such tasking, with public reasons.

5. Conducting Periodic Reviews of the Effects of Legislation

Major pieces of security legislation such as the *CSIS Act*, enacted in 1984, and the first *Anti-terrorism Act*, enacted after 9/11, have traditionally contained provisions that mandate five-year reviews by parliamentary committees. Neither Bill C-44 nor Bill C-51 requires such review, but the Senate security committee that reviewed Bill C-51 stated that it will conduct one and in its campaign pledges, the current Liberal government promised such a review.

Five-year reviews are no excuse for enacting bad laws, but they could provide warnings and help Parliament adjust laws should they produce pernicious and unanticipated effects. At the same time, however, regular parliamentary committees may have difficulties gauging the precise effects of laws unless they have access to the increasing amount of information that the government classifies as secret. For example, access to secret information will be required to assess the impact of many of CSIS's new powers. It will also be necessary to determine the effects of increased information sharing powers and provisions that make it easier to place persons on no-fly lists or revoke their passports. In our comparative analyses, we have both concluded that Parliaments in other Westminster democracies outperform Canada in reviewing and potentially enacting laws, in part because of the existence of specialized committees of parliamentarians with access to secret information and also because of independent monitors of anti-terrorism laws.[50]

Without statutory change, a committee reviewing Bill C-51 will be dependent on whatever information the government, expert watchdogs, and courts have made public about how the new security powers have been exercised. In practice, that means very little information at all. This legislative ignorance also diminishes the proficiency of parliamentarians in deliberating on the merits of new law projects, a phenomenon we believe was demonstrated in acute form in debates on bill C-51 and C-44.

50 Craig Forcese, "Fixing the Deficiencies of Parliament Review of Anti-Terrorism Law: Lessons from the United Kingdom and Australia" (2008) *IRPP Choices* 2, 14 no. 6. online: http://ssrn.com/abstract=1623472

This does not need to be the case. A CoP with access to secret information could review whether the predictions that we and others have made about the adverse effects of the new laws have come to pass, and the expertise gained by committee members could, in principle, inform deliberations of other parliamentary bodies on laws touching on national security.

C. Are there risks in creating a committee of parliamentarians?

Of course, the creation of a CoP does present challenges.

1. Lack of Trust

The most animated objection to a CoP is that parliamentarians may prove untrustworthy and may leak secret information. This fear has stalled progress on a CoP since the McDonald Commission recommended the creation of such a committee in 1981. Nevertheless, the "parliamentarians cannot be trusted argument" is an exaggerated concern, borne more of prejudice than hard data.

First, it is not justified by Canada's own history with SIRC. Many of the members of SIRC have been past provincial or federal parliamentarians. To the best of our knowledge, there has not been a breach of confidentiality in SIRC's work.

Second, this fear is belied by the experience in allied states, almost all of whom provide some secret information to at least some parliamentarians and have done so in a manner that retains the confidence of their own security services and those of allies who may share information with them. Indeed, the EU Parliament report noted that while the actual practice is often more limiting, "[t]here are a surprisingly large number of national parliaments (8) in which any MP can, in principle, have access to classified information up to an including information classified as 'Top Secret'".[51]

It follows that those who object to a Canadian CoP for fear of unreliable parliamentarians must suppose there is something particularly untrustworthy about Canadian (as opposed to foreign) parliamentarians. They must also assume that Canadian legislators are particularly

51 Wills et al, *Parliamentary Oversight*, 120.

risk-loving when it comes to criminal culpability

In this last respect, we support the idea that, like the security services, SIRC and the OCSEC, special advocates and past staff of commissions of inquiry, the members of the CoP (and its staff, and any parliamentary staffers privy to classified information) be bound by the criminal strictures of the *Security of Information Act*.

We do not believe that a CoP should enjoy parliamentary privileges, including protection from prosecution for speech that might impinge on security secrets. Immunizing parliamentarians from commonplace secrecy strictures would create uncertainty and might undermine the confidence that foreign agencies need when they frequently share information with Canadian agencies. We believe the prospect of criminal culpability, combined with a thoughtful and competent selection process, is a meaningful safeguard.

Third, we believe that the primary focus on efficacy review means in practice that the CoP review functions would be less often centred on operational conduct than is the case for propriety review, and thus the most sensitive information would not typically be at issue. To be clear: we would not deny the CoP access to operations-related information if necessary in performing its functions. It does, however, seems likely that this eventuality would be less commonplace if those functions were primarily efficacy focused.

2. Perfunctory accountability and partisanship

Politicians owe allegiances to their parties and this has a potential to distort the review process. One leading US security scholar categorizes legislative reviewers into four categories: "ostriches" (benign neglect toward S&I agencies); "cheerleaders" (boosters of S&I agencies); "lemon suckers" (sceptics of intelligence and S&I services); and "guardians" (both partners with and critics of S&I agencies).[52] Ensuring a full complement of "guardians" mitigates the risks of a CoP skewed toward uncritical boosterism, on the one hand, or visceral distrust, on the other.[53]

Partisanship is a related risk. A CoP might be less partisan than regular parliamentary com-

52 Loch Johnson, "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability," (2008) *Intelligence and National Security*, 23 no. 2: 198.

53 See discussion in Farson and Whitaker, *Accountability in and for National Security*, 37.

mittees, but there are no guarantees. There are, nevertheless, design measures that can minimize the prospects of dysfunctional partisanship. For instance, Joyce Murray's private member's bill attempted to prevent majority party domination of a new CoP by providing that no political party should have a majority of committee members. This is a worthy idea. So too is design feature in the Murray and Segal private members bill that would allow the committee to appoint its own chair, minimizing the prospect of a prime ministerial appointee controlling the committee agenda.

In the final analysis, we hope that partisanship might be muted. If serious parliamentarians undertaking a grave and serious task, outside of the limelight, prove unable to set aside their differences, that is condemnation of our system of government and the people we elect to Parliament, and not really an objection to the concept of a national security CoP.

3. Limited expertise and focus

National security is a complicated pursuit, especially when obscured by secrecy. Parliamentarians—especially those in the Commons—face challenges in mastering security matters. Even the most diligent parliamentarians, with their many other responsibilities, would struggle to stay on top of the complex and growing security file. The Canadian House of Commons has one of the highest turnover rates among democracies.[54] In consequence, our members of Parliament are less experienced in their chosen political profession than their counterparts in close allies.[55] Mitigating this difficulty enhances the need both for continuity of membership on the committee, potentially across Parliaments, and for robust and consistent staffing, permitting the accumulation and retention of expertise at the staff level. It also favours membership from the Senate—the security of tenure enjoyed by senators, properly exercised, permits the accumulation of institutional knowledge potentially of considerable value to the CoP.

54 See Richard E Matland and Donley T Studlar, "Determinants of Legislative Turnover: A Cross-national Analysis" (2004) B*ritish Journal of Political Science*, 34: 87. online: www.academia.edu/8407291/Richard_E._Matland_and_Donley_T._Studlar_Determinants_of_Legislative_Turnover_A_Cross-National_Analysis.

55 See Aaron Wherry, "Why MPs Come and Go in Ottawa" *Macleans*, January 19 2015. online: www.macleans.ca/politics/ottawa/what-to-do-with-all-the-new-in-the-house-of-commons/.

4. Confliction with expert bodies

The review system should be coordinated to minimize the risk of overlapping and competing jurisdictions among review agencies (a concept we shall describe as "confliction"). In our model, an expert review body would have in principal responsibility for propriety review and a CoP would primarily be focused on efficacy review. We agree with the Martin government paper that a CoP generally "should avoid the detailed review functions" of expert bodies.[56] Parliamentarians may not have the time or expertise to get into the weeds of actual security operations, at least as compared to executive watchdog review agencies.

On the other hand, we do not believe that CoP should be tightly corralled and statutorily excluded from inquiry into any operational matters, in the manner that exists in some other countries. For one thing, such hermetic seals simply open the door to a new sort of stove-piping. Indeed, in practice, most states do not lay out specific rules on which matters there review bodies will examine. As the EU Parliament report notes, too precise a mandate may be used by governments to corral and limit the review body,[57] something that has clearly happened in Canada's siloed and stove-piped review environment.

Moreover, a bright line between policy and operations may be unsustainable, as the two may be closely linked, as indeed the McDonald Commission emphasized. The line between efficacy and propriety review is not a certain one, and overly constraining legislative language simply opens the door to disputes over where that line lies. Rather, the legislated mandate of the CoP should orient it in the direction of efficacy review, but accept that some level of duplication of effort between the CoP and review bodies is necessary to avoid matters falling through the cracks. Some degree of overlap can also reinforce accountability.

5. Review overload

Finally, we acknowledge that Canada's S&I community is comparatively modest in size and expansive in terms of mandate. A service whose resources are disproportionately skewed to review accountability may be hard pressed to perform its core functions. Such a development would be

56 Martin discussion paper, 24.
57 Wills et al, *Parliamentary Oversight*, 103.

detrimental to security, and potentially even detrimental to review if a service is forced to make responsiveness to review a second order priority.

Part of the answer to this conundrum is to ensure that review bodies themselves manage overlapping review activities in a manner that minimizes review overload. Part of the answer is likely also a regularized relationship—a standardized review relationship will inevitably be more sustainable than a constant pattern of ad hoc commissions of inquiry. We again point to allies—particularly the similarly sized country of Australia—that are able to sustain multi-prong review structures with broader remit than Canada.

D. What design would best achieve objectives and minimize risks?

Put simply, on top of a viable mandate, there are three key ingredients for an effective CoP: good people, good resources, and good access to information. Like the Martin discussion paper and the 2004 report of the interim committee of parliamentarians on national security, we believe that achieving these objectives requires a statutory framework, as opposed to the creation of a regular parliamentary committee constituted under the standing orders of the House of Commons and Senate.

1. Good people

Everything depends on the selection of members of the committee. As the Martin government discussion paper noted, "discretion, maturity and experience are essential qualifications for membership" in a CoP.[58] Even a comparatively potent committee will provide nothing more than the illusion of accountability unless its members are willing and able to pursue the committee's functions effectively. Members must have knowledge and interest in intelligence and security and be willing and able to exercise their functions impartiality. They must be able to perform these functions in a manner that creates trust between the committee and intelligence agencies,[59] but that does not amount to regulatory "capture" by those agencies.

The requirement for expertise and institutional knowledge favours a system in which

58 Martin discussion paper, 28.
59 Wills et al, *Parliamentary Oversight*, 98.

members serve for the duration of a Parliament, and if returned after an election, are reappointed to the committee. The CoP must be able to persist and continue its work through prorogations and dissolutions, a stature that requires a legislated committee structure. The Martin government paper and the 2004 interim committee of parliamentarians favoured this approach to continuity.[60]

2. Good Resources

Staff

The CoP will also need access to facilities equipped to handle and protect classified information—this need must be taken into account in financing the CoP's work. The use of secure facilities should not compromise the CoP's independence. For example, the CoP should not be housed in facilities shared by the agencies it reviews.

Moreover, as the EU Parliament report underscores, it is "axiomatic" that review bodies have "adequate financial and human resources in order to be effective".[61] The report regards it as "essential" that the body have its own staff. Parliamentarians will, in practice, be part-time participants on the review committee, and turnover among parliamentarians will occur, especially between parliaments. A stable expert staff is required to ensure continuity and institutional knowledge, and to ensure that the committee can actually function, a point observers have made in describing performance shortcomings of the UK ISC.[62] One problem with the UK ISC, however, is that it does not have independent counsel as many other UK parliamentary committees have. A Canadian CoP should be advised by independent counsel, perhaps drawn from the ranks of security cleared special advocates, who do not have real or perceived interests in defending the legal advice that the agencies receive from Department of Justice lawyers.

We believe a CoP would be assisted in performing its tasks by the adoption of another British and Australian innovation: an independent monitor of anti-terrorism law. We describe this entity below.

60 Martin discussion paper, 29.
61 Wills et al, *Parliamentary Oversight*, 100.
62 See Peter Gill, "Obstacles to the Oversight of the UK Intelligence Community," *E-International Relations* July 19 2013. online: http://www.e-ir.info/2013/07/19/obstacles-to-the-oversight-of-the-uk-intelligence-community/.

Costs

The 2004 interim committee of parliamentarians that investigated the prospect of a CoP estimated that the operating budget (over and above costs for secure premises, translation, transcription and security clearances) of such a body would be $3 million per year—a considerable amount relative to any regular parliamentary body but modest as compared to the then-$1 billion plus budget of the S&I community. The interim committee urged that "[t]o provide anything less than this level of support would undermine the effectiveness of the committee's work. Without this commitment we question whether effective parliamentary scrutiny of the intelligence community can be achieved".[63]

Since 2004, the expansion of CSIS powers, the acceleration of RCMP national security activity, the creation of CBSA, and expanded role of CSE and enhanced all-of-government information-sharing, as well as rising threat levels, all suggest that the resource needs of a CoP will also have increased.

3. Good Access to Information

Unless the CoP has full access to classified information, it will not be able to complete its task.

This is an issue on which, however, there are considerable differences between models, in part because of the sorts of concerns discussed above under the heading of "bounded transparency".

A number of models—including that tabled as bill C-81 under the Martin government—imposed ministers as the gatekeeper on CoP access to information. In key respects, that bill was modelled on the UK ISC. In 2014, a regular UK parliamentary committee described the difficulties the ISC has faced in both in terms of receiving and sharing sensitive information. For instance, the ISC has been unable to obtain the confidential annexes in the reports of the UK's expert review bodies. The ISC has also been denied access to at least some ministerial information. It has also complained that officials testifying in front of it have not been open.[64] It remains to be seen whether this experience will be cured by the relatively modest amendments made in

63 Report of the *Interim Committee of Parliamentarians on National Security* (October 2004). online: www.pco-bcp.gc.ca/docs/information/publications/aarchives/cpns-cpsn/cpns-cpsn-eng.pdf.

64 UK Parliament, Home Affairs Committee, Seventeenth Report (2014): 82. online: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf

2013 that add more precision as when information can be refused to the committee.

In comparison to the Martin government bill and the ISC experience, the Murray and Segal bills and the recommendations of the 2004 interim committee proposed essentially unconstrained access to information (other than Cabinet confidences), analogous to that enjoyed by SIRC. We strongly support the approach taken in the Murray and Segal bill—one that declines to treat parliamentarians as more untrustworthy than expert reviewers.

We acknowledge that there are classes of information that may raise particularly acute (and legitimate) sensitivities. Information pertaining to ongoing operations fall into this category. Likewise, S&I agencies will be preoccupied with the sharing of information on sources and methods of intelligence collection, and information shared by allied agencies pursuant to (effectively automatic) non-disclosure caveats. In truth, many review bodies in counterpart democracies have limited access to these classes of information.[65]

Again, we favour SIRC-like access by the CoP. However, if there are to be limits on the CoP's access to information through an executive gatekeeper function, the limits on access to information should at least be carefully and precisely circumscribed. Possible categories of carefully codified restriction would be information: that would identify police or CSIS sources; that would compromise an ongoing operation; or which a foreign agency has shared with Canada for a limited purpose, subject to nondisclosure caveats the foreign agency has declined to waive. In other words, the executive should not have a broad discretionary power to deprive the CoP of information and any limits on access to information should be clearly prescribed and proportionate. Moreover, any restrictions should include provisos dictating the creation of summaries redacting the acutely sensitive information, but leaving in place the substantive content. This summarizing function could reasonably be performed by an expert review body—for instance, SIRC—with unalloyed access to all information (other than Cabinet confidences). Such sanitized-summary practices are relatively commonplace now in national security judicial proceedings.

Moreover, if access to information is controlled by the executive, it will necessary to create a formal dispute resolution mechanism—if conflicts emerge between the CoP and the executive over access to secret information, the matter should be resolved in front of designated judges of

65 Ibid., 124 et seq.

the Federal Court under the established procedures and jurisprudence of s.38 of the *Canada Evidence Act*.

As already argued, however, we think the better solution to the problem of acutely sensitive information is not to enumerate classes of information denied to the CoP and to task SIRC with time consuming redaction responsibilities, but instead to give the CoP access to all relevant secret information on the same grounds as SIRC. Those who remain concerned about leaks and "need to know" should be comforted by the prospect that CoP review will less regularly dwell on operational details than does propriety review and that any leaker would be subject to criminal investigation and possible prosecution.

In our model, the CoP will receive the special, classified reports prepared by the expert review bodies to ministers. These reports will obviously relate to propriety issues, and may implicate the particularly sensitive types of information. We suspect, however, that reports to the minister are themselves written in a manner that does not reveal, e.g., sources and methods. They should themselves be drafted with an eye to the "need to know" principle—in the case of expert review body reports to the minister, "need to know" for executive oversight purposes.

A related issue is how much information can the CoP then share in its own reports, a topic raised above in the context of bounded transparency. We agree that simply bringing a handful of parliamentarians inside the secrecy tent increases the size of the tent, without necessarily offering a window on activities in it.[66] An overly oblique review process would offer nothing in terms of enhanced public confidence.

We note that in 2014, a UK regular parliamentary committee raised concerns about the UK ISC's provision of information to the public. It noted that the UK ISC "compared unfavourably to both Australia's Parliamentary Oversight Committee and Canada's Security Intelligence Review Committee in terms of the level of detail included in their reports."[67]

We urge, therefore, strong legislative guidance on reporting out of the CoP, as well as a formal and credible dispute settlement regime where aspects of that proposed communication are challenged by government.

66 On this point, see Philippe Lagasse, "Should Parliament 'oversee' national security affairs," *Policy Options Magazine*, February 25 2015. online: http://policyoptions.irpp.org/2015/02/25/should-parliament-oversee-national-security-affairs/

67 UK Parliament, Home Affairs Committee, Seventeenth Report: 83.

Part IV: Fixing Expert Review in Canada: The Need for an S&I Community Reviewer

It would be an enormous mistake to proceed with a CoP without also repairing Canada's other serious review deficiency: the stove-piping and siloing of expert, propriety review. As we have suggested above, Canada needs a CoP with access to classified information, but such a committee will be limited by the other demands on parliamentarians and should generally be concerned with big picture and efficacy-related matters. Enhanced executive review and audit of the day-to-day work of the S&I community is not duplicative of the review conducted by a CoP. The CoP should focus on the big picture and questions of efficacy while the expert body will focus on specific activities and questions of propriety. The two different forms of review will nourish each other.

In broad terms, there are essentially two options for repairing the shortcomings of our present expert review problem: the Arar Commission model or some sort of "S&I community reviewer", sometimes dubbed "super SIRC" (although it such a body need not be simply an expanded SIRC). Table 3 summarizes the essence of these two proposals.

As a member of the Arar Commission's research advisory committee, one of us (Roach) supported its 2006 recommendations. A decade later, however, we are of the view that an S&I community reviewer is now necessary to renovate Canada's antiquated review structure.

First, the pattern in allied countries appears to now be firmly heading in the direction of a consolidated expert review body. Australia has a single Inspector General for Intelligence and Security for its intelligence community. The United States Privacy and Civil Liberties Oversight Board is also not stove-piped to individual agencies. And the UK is moving toward consolidating a stove-piped review and accountability regime in the area of investigatory powers into a single, independent Investigatory Powers Commissioner.[68]

Second, the former government rejected the Arar Commission's recommendations for an RCMP review body with unrestricted access to secret information and statutory gateways with SIRC when it created the CRCC. Ignoring the Arar Commission's arguments that audit-based

68 *Draft Investigatory Powers Bill* (November 2015), Chap. 8. online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

reviews (as opposed to complaints) are essential for effective review of secret national security activities, it also refused the CRCC power to conduct reviews if such reviews could not be re-sourced without detracting from the CRCC's ability to hear external complaints arising from the policing activities of almost 20,000 RCMP officers.[69] Put another way, the CRCC would need to be rebuilt anyway.

Third, nothing less than an S&I community reviewer could review information-sharing under the 2015 *Security of Canada Information Sharing Act*,[70] which allows 17 different departments (many subject to no independent review) to receive broadly defined security information. The Conservative government that enacted the law argued that the existing review structures including the Privacy Commissioner and the Auditor General were up to the task.[71] Nevertheless, this ignored the limited powers and capacity of the Privacy Commissioner and the Auditor General (concerned with government financial matters). Whatever reforms, if any, are made to this Act, it seems likely that enhanced information sharing of some sort will remain, necessitating a matching of expanded S&I community activity with expanded review.

An S&I community reviewer would take on the work of SIRC, the OCSEC and the minimal national security review work done by the CRCC for the RCMP. The goal would be a body that has jurisdiction to examine all national security matters within the federal government. This would allow the body to follow the trail of intelligence, information-sharing, and other national security activities throughout government without the need for statutory gateways. Legislative reform would be required to create this entity.

An S&I community reviewer should also be able to challenge, in Federal Court, government refusals to allow it to publish part of its reports because of secrecy concerns. Such challenges should be rare, but they would help prevent governments over-claiming secrecy. As with SIRC, we expect that the new review body would produce annual public reports and public reports on matters of interest. Its classified reports would go both to the Minister of Public Safety but also to the new CoP.

69 *Enhancing RCMP Accountability Act* S.C. 2013 c.18 Part VI.

70 S.C. 2015 c.20.

71 Government of Canada, Backgrounder to the Security of Canada Information Sharing Act (2015). online: http://news.gc.ca/web/article-en.do?nid=926879.

Table 3: Models for Reforming Expert Review

	Arar Commission Model	S&I Community Reviewer
Elements	Overcoming siloing: The OCSEC, SIRC and a new RCMP Independent Complaints and National Security Review Agency (ICRA) would be linked through "statutory gateways" facilitating the exchange of information, referrals of investigations, joint investigations and coordination of reporting. Cooperation would be enhanced by an umbrella committee, the Integrated National Security Review Coordinating Committee (INSRCC), comprising the head officials from the ICRA, SIRC and the CSE commissioner. This body would ensure the effective operation of the tripartite Canadian review mechanism.[72] Overcoming stove-piping: The CBSA, as a law enforcement-oriented entity, would be incorporated into the ICRA's mandate. Meanwhile, SIRC's functions would be expanded to include the national security activities of CIC, Transport Canada, FINTRAC and DFAIT.[73]	Overcoming siloing: A single entity—the S&I community reviewer—would subsume the existing expert review bodies. It would exercise SIRC-like review and complaints powers. Overcoming stove-piping: The entity's remit would extend to the S&I community as a whole. This broadened focus could be achieved along the model of the Australian Inspector General of Security and Intelligence by enumerating in statute the agencies subject to review. Or—our preference—the S&I community reviewer could be assigned subject matter rather than agency jurisdiction, in the same manner as the Privacy Commissioner has privacy subject matter responsibility for, effectively, all branches of the Canadian public administration.
Pros	• Preserves current institutional structures, subject to a serious revamping of the comparatively inadequate RCMP CRCC so that this body actually meets the expectations of the Arar model. • Continuity of SIRC and OCSEC reduces "growing pains" in terms of staffing, institutional knowledge, internal organization and trust building with at least CSIS and CSE. • Permits different review agencies to specialize in different areas and accommodates the potentially different roles of a review body examining police investigations and review bodies examining intelligence.	• Could follow the trail of intelligence, information sharing and other national security activities throughout government, without the need for statutory gateways between review bodies. • Would become a focal point for complaints about the government's national security activities. • Could also avoid what the Arar Commission recognized were legitimate concerns about overlapping and potentially duplicative review. • Could achieve economies of scale in terms of expertise, resources and staff, and permit full-time members (presently, both SIRC members and the CSE Commissioner are part time). • Would sidestep the need to reform the RCMP CRCC, which presently has limited powers to see secret information and has a review mission subordinated to its complaints function.

72 Arar inquiry, *Policy Report,* 8.
73 Ibid., 606.

Cons	• Even if implemented as recommended by the Arar Commission, a potentially bureaucratic and awkward solution to the siloing problem, requiring careful choreography between separate review institutions, with the accompanying risk of both gaps and duplication. • *External* information management issues stemming from ensuring that highly sensitive information associated with different agencies is only shared through the statutory gateways with review bodies on a "need to know" basis. Agencies themselves do not treat their information as an undifferentiated "whole of government" product, and share between themselves based on strict protocols. The review bodies would need to be attentive to these protocols, to avoid the liberal diffusion of agency information. • Effectively unworkable at present because the RCMP CRCC has anemic statutory powers to see secret information and therefore would be a dangerously weak link in the tripartite chain, even if it actually did begin reviewing RCMP national security activity (which, as best we know, it has not done).	• Meaningful transition costs of scaling up SIRC, while preserving core CSIS expertise, incorporating OSEC competence, and preserving review body morale and work environment. • Drafting and design issues in terms of articulating the S&I community reviewer's mandate and jurisdiction, and then start-up issues in applying that mandate/jurisdiction in practice. • *Internal* information management issues stemming from ensuring that highly sensitive information associated with different agencies is only shared internally with reviewers on a "need to know" basis. Agencies themselves do not treat their information as an undifferentiated "whole of government" product, and share between themselves based on strict protocols. The review body would need to be attentive to these protocols internally, to avoid the liberal diffusion of agency information.
Common challenges	• Building expertise on national security review of other agencies that thus far does not exist in the system anywhere. • Trust-building issues with an S&I community writ large that will need to learn to work with a new reviewer or new review environment or both.	
Relationship with the Privacy Commissioner	• At present, the Privacy Commissioner reportedly faces challenges in performing its functions in relation to national security, in part because of the silo effect. In a "statutory gateways" approach, the Privacy Commissioner should participate with the specialized review bodies in the proposed National Security Review Coordinating Committee.	• Since an S&I community reviewer would have all-of-government subject matter jurisdiction broad enough to capture privacy issues, it could be expected to perform propriety review of national security privacy and information-sharing performance. In such circumstances, the Privacy Commissioner could refer matters it discovers in its own reviews to the S&I community reviewer and this might avoid the need to give the Privacy Commissioner increased powers with respect to secret information.

Part V: Independent Monitor of National Security Law

Both the United Kingdom and Australia have a third institution dedicated to national security accountability: independent monitors of national security law.

These independent monitors are non-government lawyers with a part-time, statutory mandate to issue reports on government performance under anti-terror law and who are entitled to see secret information. But even more notably, they have also examined the necessity and usefulness of existing anti-terror laws and responded to requests to examine law reform in particular areas, creating a considerable volume of independent, thorough, and public expert policy analysis. This material has then figured prominently in subsequent parliamentary deliberations on anti-terror law. Retaining a reviewer of this sort to perform a "special rapporteur" role in offering expert input would contribute subject matter expertise to the CoP's work, and also that of regular parliamentary committees performing more classic legislative functions.

We are aware that some will criticize the addition of a monitor as duplicative of work done by a CoP and expert reviewers. If the UK and Australia have seen the need for the three forms of distinct review, however, we do not think that the case has been that Canada's security and intelligence apparatus somehow needs less review than does that in those close allies (and Westminster democracies).

In principle, one would think that Canada's existing review bodies would assist in policy deliberations by offering their views on the merits of law projects or policy proposals. SIRC once did this in the 1980s, during the mandatory five-year review of CSIS. That tradition now seems to have waned. With the exception of the Privacy Commissioner, review bodies are extremely circumspect, even ambiguous, in opining on law projects. This may reflect the fact that because they hear complaints, they view themselves as quasi-judicial, and therefore are reluctant to participate in policy making. It may also reflect the effect of operating in a security intelligence community whose culture is not conducive to the open expression of dissent from government policy.

Indeed, it is not even clear these bodies are able to express views on policy in private. Whatever the government claims in the C-51 debate to the contrary, it appears the government did

not hold advance consultations with review bodies, unless you consider notification (in general terms) consultation.

The net result is that a lot of expertise on policy matters is never communicated to executive government, let alone parliamentarians. Even if review bodies were able to discuss secret issues with a parliamentary committee empowered to hear such information, this would not necessarily translate into a more forthright discussion with review bodies on the legislative policy implications of these issues. Rather, the conversation might focus instead on the more micro-operational matters scrutinized by the reviewers.

A monitor would address, in other words, a key deficiency not fully addressed in any other way. First, this independent monitor may overcome problems of complexity and scope in national security law. With a wide-ranging mandate, an independent evaluator will identify lacunae and difficulties that might otherwise escape the attention of parliamentary committees, and place them on the official agenda. We are often struck by the independent legal expertise that is available to many of the UK parliamentary committees, although unfortunately not the ISC.

Repeated annual or special reports by an independent monitor also mitigate against the gradual normalization of national security—and especially anti-terrorism—laws and powers. In other words, it guards against the prospect that these laws will fade from media and public consciousness and lurk below the radar screen in Canada's statute books. Anti-terrorism provisions—especially those in C-51—are radical enough that they should not be left unscrutinised. This reporting may also galvanize more regular (and transparent) policy-thinking within executive government, as it appears to have done in the United Kingdom. [74]UK government responses to its independent monitor have produced a corpus of documents and discussion papers, many of which are much more informative than the guarded government reaction in Canadian legislative proceedings. Reports by an independent monitor could also assist civil society groups in this legally complex area. We note that there are reasonable disagreements in many areas of national security and research has confirmed that there has been productive tension between the

74 David Anderson QC, the current independent reviewer has prepared well over 10 reports on the annual operation of terrorism legislation, on particularly controversial powers under that legislation, on particular operations and a study of investigatory powers issues in anticipation of a government bill and legislation. See https://terrorismlegislationreviewer.independent.gov.uk

recommendations made by the first UK independent reviewer and those made by parliamentary bodies.[75]

An independent monitor might take some of the high (and low) politics out of parliamentary deliberations on anti-terrorism issues. If empowered to comment on proposed law reforms, a credible, independent evaluator should be difficult to ignore, or paint in a partisan light.

An independent monitor would have to be cognizant that his or her participation in policy debates did not detract from other duties. In this vein we note that the UK's current independent reviewer, David Anderson Q.C., has been able to comment on proposed investigatory powers bills and also commented on aspects of 2015 legislation, although we are also aware that neither the Australian or British legislation provides monitors with explicit powers to comment on bills. We recognize that there may be some risks of such comments, especially if they amount to pre-approval of laws the monitor might then assess. We consider, however, that the benefits of informed criticism outweigh these risks and that a monitor could still conclude that even properly worded legislation has nevertheless subsequently been administered improperly.

Moreover, a stable system of expert, parliamentary and independent monitor reporting, coupled with executive response and parliamentary examination, might generate a more generalized expertise in the area of national security law—so long as the government both promptly releases and responds to reports from all three review bodies. Ideas would be tested and debated in public venues, potentially allowing rapid, but reasonably carefully-vetted, responses to crises that might emerge in the future. Policy actors (well-apprised on the legal and policy terrain by the expert policy review) might have the capacity to focus not simply on hot-button issues that arise in legislated responses to crises, but also on the more detailed and complex issues that may otherwise escape scrutiny. The result may be parliamentarians—with their democratic legitimacy—possessed of the expertise that is required to question executive-driven security policies.

75 Jessie Blackbourn, "Evaluating the Independent Reviewer of Terrorism Legislation" (2012) Parliamentary Affairs 1.

Conclusion

Reform of Canada's national security review system requires three institutional pillars. Enacting one without the other two will increase the risk of important matters affecting the efficacy or propriety of national security activities (or both) slipping through the cracks. Three pronged review follows the best practices of similar countries such as Australia and the United Kingdom, and should not be dismissed as duplicative red-tape.

To summarize our views: it is long past time that Canada catch-up with other democracies in allowing a parliamentary committee to see classified information that is the regular staple of national security activities.

A statutory committee of parliamentarians will tend towards needed review of the efficacy of national security and examining how various agencies work together (or not). Such a committee with access to secret information could, for example, examine the October 2014 terrorist attacks to determine if they could have been prevented and whether new legislation enacted in response to those attacks might have made a difference. However, such a committee is almost certainly not the best tool for detailed propriety review.

It is necessary therefore, to revamp a second pillar of review: expert review. In this area, Canadians presently rely on the work of expert review bodies such as SIRC, the OCSEC, the CRCC, and the Privacy Commissioner. However, since at least the 2006 Arar Commission report, there is widespread agreement that this existing review structure is inadequate because it remains mired in silos and does not extend to many agencies such as CBSA that have important national security responsibilities. This is a situation that should not be ignored. Moreover, it should be addressed at the same time as the government moves forward with a new CoP. A stool with only one leg will be inadequate as part-time parliamentarians cannot be expected to do the same job as expert executive reviewers with full time staff.

In our view, the best option would be to consolidate expert review functions into one body that would have whole of government jurisdiction to match the government's integrated approach to national security. The Arar commission's more modest 2006 recommendations would

be better than nothing. Nevertheless, much has changed in the last decade and, in our view, the creation of statutory gateways and joint investigation powers between the existing, but siloed, bodies is now an inelegant and insufficient solution to the expanded powers and increased integration of the S&I community.

Third, we also urge the creation of a non-bureaucratic monitor on national security law following best practices in Australia and the United Kingdom. Like the other reviewers, this monitor will require access to classified information. Such a monitor could assist the new CoP and regular parliamentary committees in their work and provide independent legal expertise on contentious matters of national security law. The monitor could report on the necessity, and any required revisions, of security laws. This monitor and the S&I community reviewer could be tasked to do detailed investigations that even a well-resourced new CoP will likely be unable to reform.

The costs of a three pronged approach will not be trivial. These are, however, necessary investments—ones already made by counterpart democracies—that will help guard against the much larger costs that Canada will incur from either over-reacting or under-reacting to security threats.

Bibliography

Blackbourn, Jessie. 2012. Evaluating the Independent Reviewer of Terrorism Legislation. *Parliamentary Affairs* 1.

Canada, *A National Security Committee of Parliamentarians: A Consultation Paper to Help Inform the Creation of a Committee of Parliamentarians to Review National Security.* Ottawa, 2004. http://www.collectionscanada.gc.ca/webarchives/20060203031639/http://ww2.psepc-sppcc.gc.ca/publications/national_security/nat_sec_cmte_e.asp

Canada, *Securing an Open Society: Canada's National Security Policy.* Ottawa: Privy Council Office, 2004.

Canada, Auditor General, *2009 March Status Report of the Auditor General of Canada.* http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_01_e_32288.html#hd3a

Canada, *Backgrounder To The Security Of Canada Information Sharing Act.* 2015. http://news.gc.ca/web/article-en.do?nid=926879

Canada, Commission of Inquiry Concerning Certain Activities of the RCMP. *Freedom and Security under the Law Vol 2*. Ottawa: Supply and Services Canada. 1981.

Canada, 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, 2006.

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*, 2014.

Canada, Parliament of Canada, *Report of the Interim Committee of Parliamentarians on National Security.* October 2004. www.pco-bcp.gc.ca/docs/information/publications/aarchives/cpns-cpsn/cpns-cpsn-eng.pdf

Canada, Parliament of Canada, Senate Standing Committee on National Security and Defence. *Countering the Terrorist Threat in Canada: An Interim Report.* July 2015. www.parl.gc.ca/Content/SEN/Committee/412/secd/rep/rep18jul15-e.pdf

Canada, Parliament of Canada, Standing Senate and Defence Committee, *Vigilance, Accountability and Security at Canada's Borders.* June 2015. http://www.parl.gc.ca/Content/SEN/Committee/412/secd/rep/rep16jun15a-e.pdf

Canada, Parliament of Canada, *Standing Senate and Defence Committee, Reports and Observations on C-51.* May 27, 2015. http://www.parl.gc.ca/Content/SEN/Committee/412/secd/press/27may15-e.htm

Canadian Association for Security and Intelligence Studies. 2015. Roundtable Discussion of Accountability of Security and Intelligence Agencies. (unpublished notes summarizing the discussion prepared by the organizers in Ottawa, June 4.)

Chrétien, Jean, Joe Clark, Paul Martin, John Turner, Louise Arbour, Michel Bastarache, Ian Binnie, Claire L'Heureux Dubé, John Major, Irwin Cotler, Marc Lalonde, Anne McLellan, Warren Allmand, Jean-Jacques Blais, Wayne Easter, Lawrence MacAulay, Frances Lankin, Bob Rae, Roy Romanow, Chantal Bernier, Shirley Heafey, Jennifer Stoddart. 2015. A close eye on security makes Canadians safer. *Globe and Mail,* February 19.

Forcese, Craig and Kent Roach. 2015. *False Security: The Radicalization of Canadian Anti-terrorism*. Toronto: Irwin Law.

Forcese, Craig. 2008. 2008. Fixing the Deficiencies of Parliament Review of Anti-Terrorism Law: Lessons from the United Kingdom and Australia. *IRPP Choices 2* 14 no. 6. Montreal: IRRP.

Gill, Peter. 2013. Obstacles to the Oversight of the UK Intelligence Community. *E-International Relations,* July 19 2013. http://www.e-ir.info/2013/07/19/obstacles-to-the-oversight-of-the-uk-intelligence-community/

Johnson, Loch. 2008. The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability. *Intelligence and National Security* 23 no. 2: 198.

Lagasse, Philippe. 2015. Should Parliament 'oversee' national security affairs. *Policy Options Magazine*, February 25. http://policyoptions.irpp.org/2015/02/25/should-parliament-oversee-national-security-affairs/

Leigh, Ian. 2012. Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11, Intelligence and National Security. *Intelligence and National Security* 27 no. 5: 722.

MacIvor, Heather. 2010. The Speaker's Ruling on Afghan Detainee Documents: The Last Hurrah for Parliamentary Privilege? *Constitutional Forum* 19: 129.

MacDonald, Nicholas. 2011. Parliamentarians and National Security in Canada. *Canadian Parliamentary Review* 33.

Matland, Richard E. and Donley T. Studlar. 2004. Determinants of Legislative Turnover: A Cross-national Analysis. *British Journal of Political Science* 34: 87.

University of Ottawa. Faculty of Law. 2006. Principle 9.3. *The Ottawa Principles on Anti-terrorism and Human Rights.* http://aix1.uottawa.ca/~cforcese/hrat/principles.pdf

Segal, Hugh. 2015. Freedom and Security: The Gordian Knot for Democracies. In *After the Paris Attacks: Responses in Canada, Europe and around the Globe* edited by Edward Iacobucci and Stephen Toope. Toronto: University of Toronto Press.

United Kingdom. Parliament. House of Commons. Home Affairs Committee, *Seventeenth Report of Session 2013–14.* p. 82. http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf

Wherry, Aaron. 2015. Why MPs Come and Go in Ottawa. *Macleans,* January 19. www.macleans.ca/politics/ottawa/what-to-do-with-all-the-new-in-the-house-of-commons/

Wills, Aiden, Mathias Vermeulen, Hans Born, Martin Scheinin, Micha Wiebusch and Ashley Thornton. 2011. *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.* Brussels: European Parliament.

Wark, Wesley. 2015. Once More into the Breach: Strengthening Canadian Intelligence and Security Accountability. *Canada2020,* March. http://canada2020.ca/once-more-into-the-breach/

Whitaker, Reg and Stuart Farson. 2009. Accountability in and for National Security. *IRPP Choices 1* 15 no. 9.

Wright, Andrea. 2008. Casting a Light into the Shadows: Why Security Intelligence Requires Democratic Control, Oversight and Review. In *The Human Rights of Anti-Terrorism,* edited by Nicole LaViolette and Craig Forcese. Toronto: Irwin Law.

Appendix I: Annotated Legislation creating an Intelligence and Security Committee of Parliament

This legislation builds on C-81, S-220, and C-622. It also includes a more preliminary outline of our proposals for an independent monitor and an S&I community reviewer. It draws from the mandate of the Arar Commission to provide a new means to resolve disputes between the government and the three proposed reviewers (the new Parliamentary committee, the independent monitor and the S&I community reviewer) about what secret information seen by the reviewer can be disclosed and in what form to the public. It would oblige a large number of amendments to other statutes. We do not set those out here.

	BILL C-
	An Act to enact the Intelligence and Security Review Act and to make consequential amendments to other Acts Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:
	SHORT TITLE
Short title	**1.** This Act may be cited as the *National Security Review Act.*
	INTERPRETATION
Definition of "Committee"	**2.** The following definitions apply in this Act "activity that undermines the security of Canada" has the same definition as in s.2 of the *Security of Canada Information Sharing Act*. "Committee" means the National Security Review Committee of Parliament established by section 3. "Commission" means the National Security Review and Complaints Commission established by section 25. "Government institution" is defined in the same manner as in section 2 of the *Security of Canada Information Sharing Act*. "Monitor" means the Independent National Security Legislation Monitor established by section 19.

	Commentary: In Bill C-51's *Security of Canada Information Sharing Act*, Parliament enacted the broadest concept of national security in Canadian law, and empowered most of the public administration of Canada to share information in response to this definition. Review both in a new CoP and in a new version of the Security Intelligence Review Committee must now match this expanded breadth of national security activity, and so the review jurisdiction outlined in this Act intentionally keeps pace by extending the remit of review bodies to the agencies named as having national security functions in the *Security of Canada Information Sharing Act*.
	PART I: ***National Security Review Committee of Parliament***
Committee established	**3.** (1) There is established a committee, to be known as the National Security Review Committee of Parliament, which is to be composed of three members of the Senate and six members of the House of Commons, none of whom are ministers of the Crown or parliamentary secretaries. **Commentary**: Comparative parliamentary committees range in size from 5 to 24. Most parliamentary committees have between 10 and 15 members. Anything larger is likely to be unwieldy for an undertaking that requires access (and then close control) over secret information and would raise concerns that the "need to know" principle of security secrecy has been strained. Moreover, smaller committees may have an easier time earning the trust of the intelligence services in relation to dealing in sensitive information (EU Parliament 2011: 96). The nine members proposed by C-81, S-220 and C-622 is a reasonable number that falls within the range of analogous democracies, while also ensuring the odd number required for effective decision-making. Senate membership is particularly important in ensuring continuity to the membership and hopefully guarding against the dangers of partisanship.
Restriction on membership	(2) No more than four members of the Committee may be members of the same political party. **Commentary:** Partisanship risks negating whatever benefit a parliamentary review committee might bring to security accountability in Canada. Bill C-622's approach, reproduced above, ensures that no one party exercises a majority vote on the committee. In several European jurisdictions, opposition parliamentarians instead chair the committee and enable the chair to control the agenda in a manner that precludes governing parties from impeding review by, for instance, closing off examination of potentially embarrassing agency conduct (EU Parliament 2011: 97).
Not a Committee of Parliament	(3) The Committee is not a committee of either House of Parliament or of both Houses.

	Commentary: The new Committee will be bound by the provisions of the Security of Information Act and the Canada Evidence Act and would not be able to rely on claims of inherent parliamentary privilege and powers that were made, for example, during the Afghan detainee affair. These powers were not particularly effective with respect to the Afghan detainee affair and would create undesirable uncertainty about the keeping of secrets.
Appointment of members	**4.** (1) Members of the Committee must be appointed by the Governor in Council and hold office subject to this section until the dissolution of Parliament following their appointment.
Opposition members	(2) A member of either House belonging to an opposition party recognized in that House may only be appointed as a member of the Committee after consultation with the leader of that party.
Approval	(3) A member of either House may only be appointed as a member of the Committee after approval of the appointment by resolution of that House.
Ceasing to be member	(4) A member of the Committee ceases to be a member on appointment as a minister of the Crown or parliamentary secretary or on ceasing to be a member of the Senate or of the House of Commons.
Serving at pleasure of Parliament	(5) Subject to sub-section (4), a member of the Committee holds office during the pleasure of the House of the Parliament by which the member was appointed and may be removed by resolution supported by a majority of both the members of the government party and the official opposition in the chamber in question.

Commentary: Everything turns on the selection of members of the committee. Methods of appointment vary between democracies. In some cases, members are elected by the Parliament. In others, members are selected by party leaders or by the speaker. In some jurisdictions, the prime minister makes the appointment, after consultation with opposition parties.

Whatever the mechanism, safeguards are required to ensure that high calibre individuals are selected and the process is depoliticized to the extent possible. The role of a parliamentary security review committee is very different from a conventional committee of Parliament, where partisan agendas are publicly advanced. Security committee membership should be preserved from manipulation by governing parties inclined to favour members unlikely to be critical of current security practices or who would parlay participation for partisan advantage. It should also be designed to ensure the trustworthiness of committee members with respect to secret information.

The system proposed in S-220 and C-622, reproduced above, amounts to a tripartite arrangement that places nomination powers in the hands of the governing party, but limits absolute governing party discretion by requiring: consultation with opposition party leaders on the appointment opposition members; that the governing party be a minority on the committee; and that each member be subject to ratification by Parliament. This seems an appropriate compromise between a governing party-dominated selection process and an open-ended parliamentary selection process. No system is perfect and we acknowledge that "consultation" has sometimes been pro forma in the hands of some Prime Ministers. We are not persuaded, however, that even the most careful legislative language can overcome this problem, and ultimately depend on the good faith of the Cabinet involved.

One issue is whether members should be security-cleared. The 2004 Martin government discussion paper rejected this prospect on the basis that inquiring into the background on parliamentarians ran afoul of parliamentary privilege and the principle that the government should not be a position to influence improperly the conduct of parliamentarians. The paper warned that security clearances run the risk of the information gathered being deployed for political purposes.[76] Nor are security clearances a feature in other Westminster CoPs.

Security of tenure is also a key consideration. Simply indicating that members serve at pleasure leaves tenure at the discretion of the executive branch, something that seriously erodes committee independence. The better model is to place dismissal in the hands of Parliament itself, as is the case in Australia and the United Kingdom. Subsection 5 replicates the Australian approach, and is consistent with recommendations made by the 2004 interim committee of parliamentarians examining a Canadian CoP. The "double majority" of government and opposition parliamentarians before a CoP member is dismissed was a recommendation made by that 2004 committee.

Designation of Chair	**5.** (1) The Chair of the Committee must be elected by the members of the Committee.
Absence	(2) The Chair may designate one of the other members to act as Chair in his or her absence for a period not exceeding 45 days.

76 Martin discussion paper, 36

Voting	(3) The Chair or acting Chair may vote at meetings of the Committee and, in the case of equality of votes, also has a deciding vote.
	Commentary: The Chair will in practice likely have considerable influence over the CoP's affairs. On the one hand it is useful to have a chair with the confidence of the Prime Minister—and presumably this is the reason why the United Kingdom ISC traditionally had a chair appointed by the Prime Minister. This approach was abandoned in 2013, and in the United Kingdom and Australia, the chair is selected by the CoP itself (in New Zealand, the Prime Minister is the chair).
Procedure	**6.** Subject to this Act, the Committee may determine the procedure to be followed in the performance of any of its duties or functions.
Staff	**7.** (1) The Committee shall engage a secretary, independent counsel and any other staff that it requires, and may fix and pay the remuneration and expenses of that staff.
Facilities	(2) The Committee may secure the use of such facilities and premises as are required for it to complete its functions and to protect the security and confidentiality of information provided to it under s.17 or otherwise. **Commentary:** This deceptively short section may determine the fate of the committee. Without resources and stable staffing, the committee will fail. Bill C-81 lacked any real provision concerning staff. The language reproduced above is from bills S-220 and C-622 and we believe it to be appropriate, but that a commitment to hiring appropriate staff should be indicated by making the hiring of a secretary and staff mandatory. While it is unnecessary to specify in the legislation, staff would need to be security cleared to top secret and subject to the Security of Information Act, in the same way as are the staff of the existing expert review bodies. One of the weaknesses of the UK's ISC is that it is advised by governmental lawyers who may have a real or perceived interest in defending legal advice that the agencies under review have received from their colleagues. We have also added language on premises—in the absence of secure premises in which to conduct its work, the CoP may prove ineffective.
Service without remuneration	**8.** (1) Members of the Committee are not to be remunerated for their services in connection with the work of the Committee.
Reimbursement of expenses	(2) Members of the Committee are entitled to be reimbursed, in accordance with directives of the Treasury Board, for expenses incurred by them in connection with the work of the Committee while they are absent (a) from the National Capital Region, as described in the schedule to the National Capital Act, on days that the Senate or the House of Commons, as the case may be, is sitting; or (b) from their ordinary place of residence at any other time.
Eligibility to remain in Commons	**9.** Despite section 32 of the *Parliament of Canada Act*, no member of the Committee is ineligible to be a member of the House of Commons or to sit or vote in that House by reason of the reimbursement of expenses under subsection 8(2).

Estimates	**10.** The Chair of the Committee must annually cause to be prepared an estimate of the sums that will be required to be provided by Parliament for the payment of the salaries, allowances and expenses of the Committee during the next ensuing fiscal year, and must transmit that estimate to the President of the Treasury Board, who must lay it before the House of Commons with the estimates of the government for the fiscal year.

SECURITY AND CONFIDENTIALITY

Oath of office	**11.** Every member of the Committee and every person engaged by it must, before commencing the duties of office, take an oath in the form set out in the schedule to this Act, and must comply with the oath both during and after their term of appointment or employment.
Security of Information Act	**12.** For the purposes of the *Security of Information Act*, every member of the Committee and every person engaged by it is a person permanently bound to secrecy.
Parliamentary privilege	**13.** Despite any other Act of Parliament, members of the Committee may not claim immunity based on parliamentary privilege for the use or communication of information that comes into their possession or knowledge in their capacity as members of the Committee.
Meetings *in camera*	**14.** Meetings of the Committee must be held *in camera* whenever the Chair, or a majority of members present, considers it necessary for the Committee to do so.

Commentary: Secrecy is among the most confounding issue in discussing a committee of parliamentarians. A group of parliamentarians is being brought into the security tent, and has access to acutely sensitive information. Put bluntly, every effort to create a committee of parliamentarians in Canada to date has failed because the government of the day concluded that Canadian parliamentarians were untrustworthy. The safeguards in this section are in our view a reasonable response to what we regard as an exaggerated and unsubstantiated fear of leaking. They will mean that parliamentarians and their staff will be subject to criminal investigation and prosecution under the *Security of Information Act*, our current version of the *Official Secrets Act*. We recognize that some academics would prefer the creation of a committee that could rely on parliamentary privileges, as was done with limited success with respect to documents relating to Afghan detainees. We tend to think that such a proposal is not realistic given past reform proposals and that its benefits would be too uncertain and potentially too harmful to national security interests. We also acknowledge doubt as to whether a legislative provision could in practice limit constitutionally entrenched parliamentary privilege, such as free speech in actual parliamentary proceedings. At the very least, however, this statutory provision would make clear that the activities of the CoP itself are not clothed in privilege; that is, that they are not proceedings of Parliament.

	MANDATE OF THE COMMITTEE
Mandate	**15.** The mandate of the Committee is to (*a*) review the legislative, regulatory, policy and administrative framework for intelligence and national security in Canada for both respect for human rights and its efficacy in protecting the security of Canadians; (*b*) review the priorities, capabilities, assets and products of government institutions in relation to protecting Canada against any activity that undermines the security of Canada; (c) review government of Canada intelligence priorities, intelligence requirements and any other directions to any government institutions in relation to protecting Canada against any activity that undermines the security of Canada; (d) review organizational and strategic changes within government institutions in relation to protecting Canada against any activity that undermines the security of Canada, including the appointment of deputy heads in these organizations; (e) review the funding levels requested for government institutions in relation to protecting Canada against any activity that undermines the security of Canada; (f) inquire into any particular activity undertaken by a government institution in relation to protecting Canada against any activity that undermines the security of Canada; (g) receive unredacted copies of reports provided to Ministers by other bodies responsible for reviewing a government institution; and, (h) refer a matter to the Independent National Security Legislation Monitor under s.20 or to the National Security Review and Complaints Commission and to receive unredacted copies of than person's reports; and, (*h*) report publicly on its activities, findings and recommendations. **Commentary:** We have proposed a mandate that blends that found in bills S-81, S-220 and C-622 with the mandate recommendations made by the 2004 interim committee of parliamentarians study. We also have crafted this language to create an "all of government" remit in terms of national security activities by incorporating the broad definitional concepts found in section 2. The principal focus of the CoP is on efficacy review. However, in (f), we leave the door open to more detailed inquiries that may raise propriety issues. As argued above, we believe that an exclusive focus on efficacy issues would create a new and artificial divide, raising the prospect of gaps in the review process.

	POWERS OF THE COMMITTEE
Powers	**16**. The Committee has the power to summon before it any witnesses, and to require them to (a) give evidence orally or in writing, and on oath or, if they are persons entitled to affirm in civil matters, on solemn affirmation; and (b) produce any documents and things that the Committee deems requisite for the performance of its duties and functions.

Access to information	**17.** (1) Despite any other Act of Parliament or any privilege under the law of evidence, but subject to subsection (2), the Committee is entitled to have access to any information under the control of any part of the federal public administration that relates to the performance of the duties and functions of the Committee and to receive from their employees any information, reports and explanations that the Committee deems necessary for the performance of its duties and functions.
Prohibition against withholding information	2) No information described in subsection (1), other than a confidence of the Queen's Privy Council for Canada in respect of which subsection 39(1) of the *Canada Evidence Act* applies, may be withheld from the Committee on any grounds.
Proactive disclosure	(3) Government institutions shall convey proactively to the Committee forthwith (a) ministerial directives; (b) institutional policies, and; (c) such additional classes of institution records as the Committee may proscribe that are relevant to the Committee's mandate under s.15. **Commentary:** We have added subsection 3 to the S-220/C-622 model to encourage proactive disclosure by the S&I community. In other respects, this section follows the S-220/C-622 model which effectively gives the CoP SIRC-style access to secret information. As we argue in the discussion paper, we regard robust access to information as a "make it or break it" consideration in assessing the legitimacy of any CoP.

REPORT

Annual report	**18.** (1) The Committee must submit an annual report to the Prime Minister on reviews conducted by the Committee under section 15 during the year.
Detailed account of Committee's activities	(2) The report must include a sufficiently detailed account of the Committee's activities, findings and recommendations so as to meaningfully inform Parliament and the public on matters identified by the Committee as being of particular public interest, subject only to those exclusions that are necessary to protect the confidentiality of information related to matters of international affairs, defence or security.
Information excluded	(3) The Attorney General of Canada may, after the Chair of the Committee has been consulted, serve notice under s.38 of the *Canada Evidence Act* with respect to material in any report of the committee that it believes should not be disclosed.
Tabling in Parliament	(4) The Prime Minister must cause a copy of the report to be laid before each House of Parliament promptly on receipt and in all circumstances within the first 15 days on which that House is sitting after the Prime Minister receives the report. (5) The government shall respond to the report within 30 days of its being tabled.

Commentary: Information control will make or break this CoP. The sweet spot lies in permitting sufficient information flow to allow the CoP to be a real accountability tool but also to preclude the public disclosure of truly sensitive information. Who has the final say in redactions from the CoP's reports is a key issue. This section, drawn from the Arar Commission experience, allows an independent court, the Federal Court, to resolve disputes between the new parliamentary committee and the government about what information will be disclosed. The Federal Court will balance the competing interests and have the option of authorizing full or partial disclosure or upholding the government's claims that the interests in non-disclosure outweigh those in favour of disclosure. We are told that in Australia, delayed tabling of the independent monitor's reports by the government has proven problematic, and so have included language putting an outer limit on tabling of the CoP's report, with a requirement that faster tabling is the default.

Information sharing with other reviewers

19. If on reasonable grounds the Committee believes it necessary for the performance of any of its functions under this Act, those of the National Security Review and Complaints Committee or the Independent National Security Legislation Monitor, the Committee may convey any information which it itself is empowered to obtain and possess under this Act to the National Security Review and Complaints Commission and the Independent National Security Legislation Monitor.

Commentary: These provisions provide "statutory gateways" to enable the sharing of secret information in this case between the new Parliamentary committee, the expanded National Security Review and Complaints Commission, and the Independent National Security Legislation Monitor. Such sharing will help ensure that the new Parliamentary committee works in tandem with the expanded version of the National Security Review and Complaints Commission, and the Independent National Security Legislation Monitor to maximize governmental accountability for those national security activities that must remain secret. This section is replicated for the other bodies below.

PART II
Independent National Security Legislation Monitor

Appointment

20.(1) The Governor in Council shall appoint an Independent National Security Legislation Monitor to hold office on a part-time basis, during good behaviour, for a term of not more than five years.
(2) Before appointing the monitor, the Prime Minister of Canada must consult with the chair of the committee.
(3) The monitor shall be a member in good standing of the bar of a province, not be employed in the federal public administration, and not otherwise be associated with the federal public administration in such a way as to impair their ability to perform his or her functions under section 20.
(4) The monitor is entitled to be paid, for each day that the monitor performs duties and functions under this Act, such remuneration as is fixed by the Governor in Council and shall be paid reasonable travel and living expenses incurred by the member in the performance of those duties and functions.
(5) The Minister of Justice shall ensure that the monitor is provided with adequate administrative support and resources.

Commentary: These provisions are a composite of the Australian *Independent National Security Monitor Act 2010*, the provisions in the *Immigration Refugee Protection Act* relating to the selection of and support given to "special advocates", and the provisions in the CSIS Act relating to remuneration for SIRC members.

Mandate

21.(1) The monitor has the following functions:
(a) to review, on his or her own initiative, the operation, effectiveness and implications of:
(i) Canada's proposed or actual antiterrorism and national security legislation; and
(ii) any other proposed or actual law of Canada to the extent that it relates to Canada's antiterrorism and national security legislation;
(b) to consider, on his or her own initiative, whether any legislation mentioned in paragraph (a):
(i) contains appropriate safeguards for protecting the rights of individuals; and
(ii) remains proportionate to any threat of terrorism or threat to national security, or both; and
(iii) remains necessary;
(c) if a matter relating to antiterrorism or national security is referred to the monitor by the committee or the minister —to report on the reference;
(d) to assess whether Canada's counter antiterrorism or national security legislation is being used for matters unrelated to terrorism and national security.
(2) If a matter is referred to the monitor by the committee, the monitor may perform the function set out in paragraph (1)(a) or (b) in relation to the matter.

	Commentary: This provision largely reproduces the core mandate of the Australian monitor under the *Independent National Security Monitor Act 2010*. However, we have expanded the scope of this function to include not just existing, but also proposed, legislation. Opposition parties in Australia have raised such an idea. It is not without controversy, since it means that the monitor may opine on laws that he or she may then be obliged to critique in their actual operation, creating concerns about whether the monitor would be compromised. On balance, however, we think that the net benefit of a recognized non-partisan expert participating in deliberations over bills outweighs this concern. We note also that vigorous and important involvement of the UK independent reviewer in current debates over the UK investigative powers bills.
Report	**22.**(1) On completion of a review under section 21, the monitor shall provide the Prime Minister and the committee with his or her report, which is to contain the findings of the review and any recommendations that the monitor considers appropriate. (2) By March 31 of each year, the monitor shall provide to the Prime Minister and the committee an annual report that contains sufficiently detailed account of the his or her findings and recommendations during the fiscal year so as to meaningfully inform Parliament and the public on matters identified by the monitor as being of particular public interest. (3) The Attorney General of Canada may, after the monitor has been consulted, serve notice under s.38 of the Canada Evidence Act with respect to material in an annual report that it believes should not be disclosed
Tabling in Parliament	(4) The Prime Minister must cause a copy of any review or report under this section to be laid before each House of Parliament promptly on receipt and in all circumstances within the first 15 days on which that House is sitting after the Prime Minister receives the report.
Powers	**23.** In performing his or her functions, the monitor has the same powers and access to information as the committee under section 16 and subsections 17(1) and (2).
Information sharing with other reviewers	**24.** If on reasonable grounds the monitor believes it necessary for the performance of any of its functions under this Act, those of the National Security Review Committee of Parliament or the National Security Review and Complaints Commission, the monitor may convey any information which it itself is empowered to obtain and possess under this Act to the National Security Review and Complaints Commission and the National Security Review Committee of Parliament
Oath of office	**25.** Before commencing the duties of office, the monitor shall take an oath in the form set out in the schedule to this Act, and must comply with the oath both during and after their term of appointment or employment.
Security of Information Act	**26.** For the purposes of the *Security of Information Act*, the monitor is a person permanently bound to secrecy. **Commentary:** Sections 22 to 24 replicate similar provisions relating to the CoP, as well as organizing the manner in which monitor reports are provided to the CoP and executive, and made public.

PART III
National Security Review and Complaints Commission

	Commentary: What follows is a partial outline of a S&I community reviewer, sometimes colloquially called a "super SIRC". Many of the details would need to be fleshed out, but could be borrowed from the SIRC provisions found in the current CSIS Act.
National Security Review Commission	**27.**(1) There is established a commission, to be known as the National Security Review Commission, consisting of a Chair and not less than two and not more than four other members, all of whom shall be appointed by the Governor in Council from among members of the Queen's Privy Council for Canada who are not members of the Senate or the House of Commons, after consultation by the Prime Minister of Canada with the Leader of the Opposition in the House of Commons and the leader in the House of Commons of each party having at least twelve members in that House. (2) Each member of the commission shall be appointed to hold office during good behaviour for a term not exceeding five years. (3) At least one member of the commission shall be a supernumerary judge or a retired judge of a superior court. (4) The Chair of the Commission shall be a full-time appointment who is entitled to the composition that is paid to a superior court judge. **Commentary:** This augments the SIRC arrangement by making the Chair position fulltime, and it draws on the OCSEC to ensure that there is at least one experienced jurist on the commission. (5) Other member of the Commission are entitled to be paid, for each day that the member performs duties and functions under this Act, such remuneration as is fixed by the Governor in Council and shall be paid reasonable travel and living expenses incurred by the member in the performance of those duties and functions. **27.** (1) The Chair of the Commission is the chief executive officer of the Committee. (2) The Chair of the Review Commission may designate another member of the Commission to act as the Chair in the event of the absence or incapacity of the Chair. **28.** The Commission may, with the approval of the Treasury Board, (a) engage a secretary and such other staff as it requires; and (b) fix and pay the remuneration and expenses of persons engaged pursuant to paragraph (*a*). **29**. Every member of the Review Commission and every person engaged by it shall comply with all security requirements applicable by or under this Act to an employee and shall take the oath of secrecy set out in the schedule. **Commentary:** These provisions replicate the structure found for SIRC in the existing CSIS Act.
Functions of the Commission	**30.** The functions of the Commission are: (1) to review, on its own initiative or on the request of a Minister with responsibility over a government institution or the committee or parliamentarians, generally the performance of any government institution in relation to protecting Canada against any activity that undermines the security of Canada.

	Commentary: These provisions create a "super SIRC" or "S&I community reviewer" that is not stove-piped or siloed. Its remit is modelled on SIRC's present open-textured language. In principle, this language reaches efficacy review. As noted above, we see the expert review body's role as principally focused on propriety review. We believe, however, that the expert body (especially with a full time chair and an expert and dedicated staff) will be able to explore "in the weeds" in a way that the CoP even assisted by staff. The super SIRC's mandate should allow it to pursue efficacy issues that it may encounter in its detailed work, in order to better report in a manner that might be useful to a CoP. Constraining the expert review body firmly to propriety review may otherwise create a new "silo"—this time between the expert review body and the CoP. (2) to hear complaints concerning the performance or conduct of any government institution in relation to protecting Canada against any activity that undermines the security of Canada as well as complaints in relation to the granting by the government of security clearances **Commentary**: The Commission would assume the jurisdiction to hear complaints against CSIS under s.41 of the CSIS Act, complaints relating to the denial of security clearances under s.42 and complaints in relation to the any government institution's conduct in relation to protecting Canada against any activity that undermines the security of Canada. This would mean that the new S&I community reviewer would continue to hear complaints against CSIS but would also hear complaints in relation to the national security work of any governmental institution in the exercise of its national security function. This would include complaints in relation to the national security work of the RCMP, CBSA and CSE. There is an argument in favour of separating review and complaints functions. We see the merits of both the fused and separated function, and are neutral on this question.
Access to information	**31**. Despite any other Act of Parliament or any privilege under the law of evidence, but subject to subsection (b), the Commission is entitled (a) To have access to any information under the control of the government that relates to the performance of any government institution in relation to protecting Canada against any activity that undermines the security of Canada. (b) No information described in subsection (a), other than a confidence of the Queen's Privy Council for Canada in respect of which subsection 39(1) of the *Canada Evidence Act* applies, may be withheld from the Committee on any grounds

Commentary: This provides the new S&I community reviewer with access to secret information on the same basis as the present SIRC receives information under s.39 of the CSIS act but with the expansion to apply to all information held by government institutions in performing their duties to protect Canada against any activity that undermines the security of Canada. This proposal is based on the principle that review powers should match the broadest security powers in this case found in the Security of Canadian Information Sharing Act enacted as part of Bill C-51. In particular, it would mean that the new Commission would have direct access to secret information about the national security work of the RCMP in a way that is denied in the *Enhancing RCMP Accountability Act*.

Information sharing with other reviewers	**32**. If on reasonable grounds the Commission believes it necessary for the performance of any of its functions under this Act, those of the National Security Review and Complaints Committee or the Independent National Security Legislation Monitor, the Committee may convey any information which it itself is empowered to obtain and possess under this Act to the Independent National Security Legislation Monitor and the National Security Review Committee of Parliament. **Commentary:** This provides the same statutory gateway language as exists for the Committee and the monitor and follows the Arar Commission in recognizing the need for review bodies to be able to share secret information so that they can more effectively work together.

SCHEDULE

(Section 12)

SCHEDULE

(Section 11)

OATH

I, ..., swear (*or* solemnly affirm) that I will faithfully and impartially to the best of my abilities perform the duties required of me as a member (*or* an employee) of the Intelligence and Security Committee of Parliament. I will not, without due authority, disclose or make known to any person any information acquired by me by reason of the duties performed by me as a member (*or* an employee) of the Intelligence and Security Committee of Parliament.