THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Bill C-59 – *National Security Act, 2017*

CANADIAN BAR ASSOCIATION

January 2018

500–865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Criminal Justice, Immigration Law, Charities and Not-for-Profit Law, Military Law, and Privacy and Access to Information Law Sections, with assistance from the Legislation and Law Reform Directorate at the CBA office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the Canadian Bar Association.

TABLE OF CONTENTS

Bill C-59 – *National Security Act, 2017*

Bill C-59 – *National Security Act, 2017*

EXECUTIVE SUMMARY

Bill C-59, *National Security Act, 2017*, proposes complex major updates to national security law. It would address decisions of the Federal Court of Canada, amendments to other national security legislation and widespread concerns expressed about Bill C-51, *Anti-Terrorism Act, 2015*.

The Canadian Bar Association (CBA) generally supports the goals and structure of Bill C-59 as a positive change, modernizing the legal framework for Canada's national security infrastructure and increasing transparency, oversight and review, features that have previously been lacking. Our comments and analysis of the proposals in Bill C-59 are offered in hopes of further improving the Bill.

National Security and Intelligence Review Agency

The CBA has previously called for a review agency with a mandate covering the entire national security apparatus. To achieve coordination and cooperation between involved government agencies, the mandate of that review body should not be restricted to a single agency. We support the creation of the National Security and Intelligence Review Agency (NSIRA) and its responsibility for broad review of the national security infrastructure as a whole but suggest amendments to the wording and structure of some sections of the proposed Act.

National Security and Privilege

The proposed *NSIRA Act* would create a new agency with access to any information (other than a Cabinet confidence) that it 'deems necessary' to conduct its work. This would extend to information subject to solicitor-client privilege, professional secrecy of advocates and notaries, or litigation privilege, creating an open-ended mechanism to review the legal advice given to government.

The principles of solicitor-client privilege apply with equal force to a government client, and the government must be able to obtain professional legal advice without the chilling effect of potential disclosure of its confidences. The quality of its legal advice would inevitably be compromised if the confidentiality of its solicitor-client communications cannot be assured. Courts have long recognized that protecting the solicitor-client confidences of government promotes the public interest by enhancing application of the law and maintaining the rule of law over public administration.

We encourage reconsideration of the proposal to do away with privilege in matters of national security or intelligence. While the Bill does seek to protect disclosed information against claims of waiver and ensure that privileged information does not find its way into certain reports (section 53), these measures miss the underlying rationale for protecting the privilege.

What constitutes a threat to national security is often subjective and has been used to justify abuse of civil liberties. The Supreme Court of Canada has recognized a limited public safety exception. The CBA believes that the case against a national security exception is particularly strong in the circumstances of the Review Agency, which largely addresses *post facto* oversight.

We recommend that Bill C-59 not include open-ended access to all records, including those subject to solicitor-client privilege.

Intelligence Commissioner

The CBA supports the creation of an independent, specialized office for the oversight and authorization of activities by the Communications Security Establishment (CSE) and Canadian Security Intelligence Service (CSIS). While we have generally called for judicial oversight, we recognize the advantages of a dedicated Commissioner with staff and resources to allow effective ongoing oversight.

The nature of the review mandated by sections 14 to 21 of the proposed *Intelligence Commissioner Act* (*ICA*) would lead to nested findings on a reasonableness standard. It suggests some deference to the Minister's initial opinion that a 'reasonable grounds' standard has been met. However, what it means for the Commissioner to find that the Minister's finding of 'reasonable grounds' is reasonable is unclear. Courts are struggling with the application of the deferential standard of 'reasonableness review' in the administrative law context. There are ongoing debates about the level of deference implied by the reasonableness standard, and whether deference applies to interpretations of law. Framing the Commissioner's review in terms subject to this debate is unnecessary and could change the Commissioner's role as jurisprudence around standards of review evolves.

These concerns could be addressed by framing the Commissioner's oversight as other applications for judicial authorization. Section 35 of the proposed *Communications Security Establishment Act* (*CSE Act*) and associated sections of the *ICA* could be amended to require that the Minister may issue an authorization if the Intelligence Commissioner concludes there are reasonable grounds to believe the relevant criteria have been met. The reasonable grounds standard is well established in many areas of law, stable and relatively well understood. Similar amendments should be considered for the *CSIS Act* and related provisions.

Communications Security Establishment

The proposed *CSE Act* gives explicit authority for certain activities now only implicitly permitted under the *National Defence Act* (*NDA*), and creates a regime of clear conditions and restrictions, including privacy protections, for the exercise of those authorities. The CBA supports the goals of greater clarity, transparency and oversight exhibited by the proposed legislation.

In addition to prior review of certain authorizations by the Intelligence Commissioner, Bill C-59 proposes that all CSE activities would be reviewed by the proposed NSIRA for lawfulness and to ensure that the CSE's activities are reasonable, necessary and comply with ministerial directions. The NSIRA would serve as the review body for complaints against the CSE.

The CBA supports the creation of the NSIRA and its review role. We also support the creation of the office of the Intelligence Commissioner and commend the government for integrating a mechanism for independent oversight and prior authorization for many of the most intrusive activities of the CSE. Section 35 of the *CSE Act* and associated sections of the *ICA* should be amended to require that the Minister may issue an authorization if the Intelligence Commissioner concludes there are reasonable grounds to believe the relevant criteria have been met.

The CBA generally supports the more detailed mandate in the proposed *CSE Act*, which increases transparency and clarity for those working for the CSE and the public more generally. Apart from extending authority for cybersecurity and information assurance activities to non-

governmental organizations under category (iv), it seems the CSE could conduct all the listed activities under the current *NDA*. Still, the clarity of the proposed list adds precision as to the scope of the mandate.

Several elements of the proposed mandate are inherently in tension with each other, for example, offensive and defensive cyber operations. While there are compelling reasons for having the same agency address both operations given the overlapping nature of the underlying expertise and knowledge base, robust mechanisms are needed to resolve this tension.

In contrast to the activities of CSIS which may address both domestic and international security, the focus of the CSE is on activities of foreign entities and individuals. The Act acknowledges – and, apparently, expressly permits – the CSE to collect personal information about Canadians or people in Canada, incidental to its activities related to foreign intelligence gathering and cybersecurity and information assurance operations. The requirement for privacy protection measures is quite general, presumably anticipating that it will be further developed through policies and procedures. Yet there is no express requirement for policies or procedures to be adopted. Any authorization for the CSE to conduct cybersecurity and information assurance operations must specify the conditions or restrictions that the Minister considers advisable to protect the privacy of Canadians and people in Canada. The Governor in Council may make regulations about the privacy protection measures required to be adopted by the CSE, but there is no requirement to make those regulations.

The *CSE Act* requires that the CSE apply privacy protection measures to all its activities, but does not require those measures to be written, publicly available policies and procedures. The CSE should develop and publish policies and procedures articulating the privacy protection measures it will apply in its operations, either by regulation power or ministerial direction.

While the *CSE Act* largely pre-empts the *Privacy Act*'s application by granting express authority to collect personal information, *Charter* protections supersede that and apply to all CSE operations (in addition to the privacy protections in the *Act*.) While this overriding protection may be assumed, a preamble similar to that in the *CSIS Act* should be added to the *CSE Act*.

The *Act* allows general disclosure of information collected through CSE operations to people designated by the Minister, and that disclosure could include personal information. It may be made only if the information is essential for international affairs matters, including security and national defence (resulting from foreign intelligence gathering operations), or necessary for purposes of protecting information and cybersecurity infrastructures (resulting from cybersecurity and information assurance operations). The CBA supports the stipulation that disclosure must be 'required' or 'necessary', and not simply 'relevant' for those purposes. The guiding principles articulated in the *Security of Canada Information Sharing Act* (SCISA), should also expressly apply to any sharing by the CSE.

Canadian Security Intelligence Service Act

The CBA expressed serious concerns about introducing threat disruption powers to the *Canadian Security Intelligence Service Act* (*CSIS Act*) in Bill C-51, *Anti Terrorism Act, 2015*. Bill C-59 would address many of those concerns.

Section 21.1(1.1) explicitly states what threat reduction measures may be taken, clarifying the scope of the activities envisaged. However, we remain concerned that the proposed kinetic powers move CSIS from the intelligence role it was designed to play.

While the regime for unlawful conduct proposed in section 20.1 would be subject to review, oversight and increased transparency, the similarity of the regime to mechanisms in the *Criminal Code* only highlights the changing mandate and nature of CSIS.

Changes to sections 12.1(2) and (3) would clarify that measures must comply with the *Charter*, addressing a primary concern we raised in previous submissions. However, section 12.1(3.2) still suggests that fundamental rights can be curtailed based on issuance of a warrant. Aside from authorizing searches under section 8 of the *Charter*, warrants cannot alter the constitutionality of state activities impinging on substantive *Charter* rights. If the proposed actions are a reasonable limit on *Charter* rights (other than those under section 8), judicial authorization is little more than a ruling to that effect. If this is the intent of the proposed amendments, it should be clear.

In light of the Federal Court ruling in *XXX*[1], and the CBA's response to the federal government's Green Paper on National Security, we welcome the new regime and generally approve of the mechanisms proposed for implementation. However, further consideration must be given to the need for a dual administrative and judicial mechanism for data. The new regime should operate based on judicial authorization, keeping with the spirit of current sections 21 and 21.1 of the *CSIS Act.*

Bill C-59 proposes new sections (beginning at section 11.01) that directly respond to the Federal Court ruling on metadata and associated data, specifically permitting CSIS to collect data not necessarily related to a threat to the security of Canada. We generally support different procedural and substantive mechanisms and safeguards, including those aimed at protecting privacy. However, we also support greater oversight by the courts for those administrative mechanisms.

Bill C-59 addresses several issues in the Federal Court ruling largely by moving away from the standard in section 12(1) of the *CSIS Act* that limits collection "to the extent that it is strictly necessary" to apply to the *collection, analysis* and *retention* of information gathered by CSIS during its investigation of activities that, based on reasonable suspicion, constitute a threat to national security. Bill C-59 substantially lowers the threshold for retaining Canadian datasets. Retention can be authorized if it is 'likely' to assist CSIS in the performance of its primary duties or functions, a lower standard than 'strictly necessary'.

In our view, the standard of likelihood is insufficient to protect the expectation of privacy for state retention of datasets related to Canadians or people in Canada. The procedural safeguards in the application include the obligation for CSIS to set out "any privacy concern which, in the opinion of the Director or the designated employee who makes the application, is exceptional or novel". The CBA supports this safeguard, also subject to terms and conditions imposed by the judge in the public interest. The Bill confers a right of appeal on CSIS if the designated judge refuses to issue the requested judicial authorization.

Again, once an authorization has been issued, CSIS may query and exploit the retained Canadian datasets. However, the querying and exploitation must *assist* CSIS in the performance of its primary duties and functions and must also be done "to the extent that it is strictly necessary". This standard has been in section 12(1) since CSIS was created in 1984, and the Federal Court ruling made clear that it covers not only the collection, but also the analysis and retention of information gathered by CSIS.

---

1 *In the Matter of an Application by XXX for Warrants Pursuant to Sections 12 and 21 of the CSIS Act,* 2016 FC 1105.

The CBA believes it is appropriate for this standard to also apply to the querying and exploitation of Canadian datasets. However, we again question whether the standard of being 'strictly necessary' should also apply to data retention as a condition for judicial authorization.

The proposed regime includes varying standards based on whether the activity is querying, exploitation, retention or the function or duty to be performed by CSIS. These subtle nuances, given the complexity of the proposed regime, could lead to debate and controversy, although the standards concerned are of no apparent operational relevance.

We have questioned the need for Parliament to establish an administrative information collection regime, instead of a system where a designated judge must approve the collection of information as part of the issuance of warrants. It would be simpler to allow the designated judge to authorize CSIS to collect certain types of data as part of the warrants granted by the Federal Court under the current section 21.

The scale and complexity of the various provisions demonstrate Parliament's will to modify the data collection system to reflect technological progress and developments in case law, primarily the Federal Court ruling. We support these changes and adaptations. Our comments are aimed at mitigating future disputes and promoting smooth application of the law, especially about the interaction between the administrative and judicial review mechanisms. The regime requires a fine balance between national security requirements and the value of privacy, constitutionally enshrined in the *Charter*. The key question is whether the balance in Bill C-59 meets constitutional standards.

Security of Canada Information Disclosure Act

The CBA has previously commented on SCISA, as it is now named – to be renamed the *Security of Canada Information Disclosure Act* – and we continue to have many concerns.

We remain concerned with the breadth of the definition of "activity that undermines the security of Canada" in section 2 and with having different definitions of national security in different parts of Canadian law. Notably, the definition in section 2 of *SCISA* is substantially broader than the definition of "threats to the security of Canada" in section 2 of the *CSIS Act*.

Bill C-59 appears intended to restrict the definition of "activity that undermines the security of Canada" by varying the list of examples. However, the list is still not restrictive. While the CBA welcomes more restrictive language surrounding some of the examples, the amendments do not clarify the intended scope of *SCISA*. A clear, restrictive definition would give both clarity and transparency on a broad disclosure regime with substantial privacy implications.

The amendment to the exception in section 2(2) is troubling, as it substantially reduces the protection under the current version. Several legitimate political activities might be seen on their face as undermining the "sovereignty" or "territorial integrity" of Canada.

The CBA supports the principles guiding information disclosure in section 4 of *SCISA*. However, to be effective, *SCISA* must include a robust oversight and accountability mechanism to enforce them, independent from the government institutions that will be sharing or disclosing information. We expect that the mandate of the National Security Committee of Parliamentarians proposed under Bill C-22 would have a similarly broad application. The CBA supports these review mechanisms and considers them to be a substantial improvement on the current situation.

The CBA has also recommended that Schedule 3 list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes they supervise or implement that might relate to national security concerns. We recommend guidelines for institutions on what is actually needed, to prevent oversharing or over disclosure of information. Receiving institutions must have obligations to destroy information they receive that is not relevant.

The record keeping requirements in proposed section 9 do not require institutions to document how security interests are being weighed against privacy interests in the context of section 5(1) of *SCISA*. The CBA recommends including this information.

Secure Air Travel Act

The CBA has expressed concerns over the practical functioning of secure air travel measures in the past, as well as preclearance measures. The need for safe air travel must not be considered super-ordinate to *Charter* values or other Canadian rights and freedoms. Any measures toward that goal must be implemented in a clear, understandable and practical way so people and businesses (particularly airlines) affected know how to deal with rights and responsibilities. While the Bill offers some improvements, it will do little to promote safe travel, negatively affect legitimate travel and commerce and provide questionable effective recourse for those harmed by its operation.

In a free and democratic society, people have a right to go about their business undisturbed by state intervention. The proposed changes cast a very wide net. The bill does not require sufficient Parliamentary scrutiny of the information collected, sets a low bar for gathering information and does not appear to stop its wide dissemination. With the number of people already wrongly placed on no-fly lists, at a minimum there should be greater scrutiny of the type of information collected, the standard to be met before it is disseminated and protections against its misuse.

In our view, steps are needed to ensure that any information gathered by regulation serves to narrow those on this list and not interfere with the legitimate travel of Canadians and businesses. Similarly, the legislation should outline the sort of information that can be gathered by regulation with some specificity and narrow the category of information that can be gathered under this power. Finally, people must have effective recourse to judicial review of any decision to deny their travel.

Criminal Code amendments

Given the significant implications of association with an entity listed under section 83.05, the criteria for the Minister to recommend listing an entity should be transparent, reviewable and regularly verified. Bill C-59 changes the relevant timeframe for entities under section 83.05(1)(b) to those who have historically acted in association with a listed entity. Given the historical nature of both sections, it is unclear how, once an entity was listed, it would ever be removed from the list. This concern also arises for the greater restrictions on reviews under section 83.05(2), which only allow review of historical evidence in relation to an entity, regardless of the passage of time.

The CBA has a related concern with proposed section 83.05(8.1), which increases the period in which the Minister must review whether there are still reasonable grounds for an entity to be listed from two to five years. More frequent review is imperative.

In 2015 and 2017, the CBA took the position that section 83.221, Advocating or Promoting Terrorism, is overbroad, vague and contrary to the core principle that the criminal law must be certain and definitive. Further, the section requires only that the accused be reckless that a terrorism offence may be committed. This low *mens rea* could be interpreted as a violation of section 7 of the *Charter*.

The offence would now be restricted to individuals who counsel another person to commit a terrorist offence. Although the existing extensive case law for 'counselling an offence' could help in addressing these concerns, distinguishing terrorism offences from general counselling offences in the *Criminal Code* creates the possibility of disproportionate application, especially for people and groups that tend to be frequently associated with terrorism.

The changes appropriately address some constitutional concerns. Clause 143 of the Bill addresses many CBA concerns by replacing section 83.221 entirely. The proposed offence consists of counselling another person to commit a terrorist offence. As the offence of counselling already exists in the *Criminal Code*, we question whether the new offence would add further protection for Canadians.

Prior to Bill C-51, the *Criminal Code* allowed peace officers to arrest and detain people on reasonable grounds to believe that a terrorist activity *will* be carried out and reasonable grounds to suspect that imposing a peace bond *is necessary* to prevent the terrorist activity. Bill C-51 replaced reasonable belief that "terrorist activity *will* be carried out" with a reasonable belief that terrorist activity "*may* be carried out". It also replaced the requirement that a recognizance or arrest of a person "is necessary to prevent the carrying out of the terrorist activity" with "*is likely* to prevent the carrying out of the terrorist activity."

The previous wording "will" and "necessary" along with the requirement of "reasonable grounds to believe" and "proof on balance of probabilities" was adequate for judges to balance societal protection with individual liberty. Bill C-51 upset this balance and Bill C-59 should rectify this problem.

The CBA welcomes the repeal of sections 83.28 and 83.29, on investigative hearings and related arrests. Proposed amendments to section 83.3 are consistent with the CBA's recommendation that the previous thresholds for recognizances and related arrests – lowered in Bill C-51 – be restored.

Youth Criminal Justice Act

The CBA supports proposed changes to the *Youth Criminal Justice Act* in Bill C-59, which would help ensure that youth charged with terrorist-related offences, or subject to terrorist-related peace bond proceedings, receive the enhanced procedural protections afforded under the *Act*.

Review

Section 168 of Bill C-59 mandates a comprehensive review of the Act "in the sixth year after the Bill comes into force" by Parliament. The review of Bill C-59 would be aligned with that of Bill C-22. If the bills come into force within a year of each other, the reviews could take place at the same time and by the same committee or committees. The CBA generally supports the comprehensive review.

Impact on Charities

The interplay between existing laws and the broad audit and sanction capabilities of CRA have resulted in significant problems for charities acting in conflict zones. They have impeded

charities' ability to demonstrate effective control over charitable assets and programs to avoid placing the organizations and their directors, officers, employees and volunteers at risk.

Bill C-59 would amend the recently enacted *SCISA* and rename it the *Security of Canada Information Disclosure Act*, emphasizing that the Act addresses only disclosure of information and not its collection or use. This is a positive step. Other amendments focus the definition of 'activity that undermines the security of Canada' and codify that advocacy, protest, dissent or artistic expression will not generally be considered to fall under 'an activity that undermines the security of Canada', narrowing the Act's application in a way the CBA supports. However, the Bill also seems to propose expanding its application by adding 'threaten' to the definition.

The proposed *Criminal Code* amendments on listed entities would change little procedurally, but would change the focus of the Minister's recommendations to the Governor in Council from recommending removal of a listed entity to recommending that the entity remain a listed entity. Information considered on judicial review of the Minister's decision would be expanded to include information considered by the Minister in rendering the decision and may still be heard in the absence of the entity or its legal counsel.

Section 83.221 of the *Criminal Code* would be replaced, changing the offence from 'advocating or promoting commission of terrorism offences' to 'counselling'. Like the facilitation offence, the new counselling offence could unduly expose charities and their boards to prosecution for charitable activities if they happen to be portrayed negatively.

More detailed analysis and recommendations are throughout our extensive submission.

Bill C-59 – *National Security Act, 2017*

I. INTRODUCTION

The Canadian Bar Association (CBA) appreciates the opportunity to comment on Bill C-59, the *National Security Act, 2017*, which was tabled in the House of Commons on June 20, 2017. The Bill proposes complex major updates to national security law in light of various decisions by the Federal Court of Canada, recent amendments to several laws pertaining to national security and concerns expressed about Bill C-51, the *Anti-Terrorism Act, 2015*.

The CBA has offered its views and expertise at many stages in the development and critique of Canada's national security and anti-terrorism regime[2] and we remain committed to contributing going forward. As suggested by the Preamble to Bill C-59, the CBA also stresses that protecting the safety and security of Canadians and preserving Canada's constitutional values are both fundamental responsibilities of the federal government.

We generally support the goals and structure of Bill C-59. We see the Bill as a positive change, modernizing the legal framework for Canada's national security infrastructure and increasing transparency, oversight and review, where those things were previously lacking. In this submission, we offer comments and concerns about aspects of the proposed framework, generally following the order in the Bill. We remain willing to engage in further discussion about relevant amendments and improvements.

II. NATIONAL SECURITY AND INTELLIGENCE REVIEW AGENCY

Bill C-59 proposes the *National Security and Intelligence Review Agency Act* (*NSIRA Act*), to repeal sections of the *Canadian Security Intelligence Service Act* (*CSIS Act*) and establish a new National Security and Intelligence Review Agency (NSIRA). In consultations and submissions on previous legislation, the CBA has called for the creation of a review agency with a mandate covering the entire national security apparatus. Given the need for coordination and cooperation amongst the government agencies engaged in national security related work, the mandate of a review body should not be restricted to a single agency. While we continue to have concerns that some agencies (notably the Canada Border Services Agency (CBSA)) have

---

2 For a few examples, see our submissions on *Bill C-36, Anti-Terrorism Act* (Ottawa: CBA, 2001), *Three Year Review of the Anti-Terrorism Act* (Ottawa: CBA, 2005), *Policy Review of the Commission of Inquiry in relation to Maher Arar* (Ottawa: CBA, 2005) and *Bill C-51, Anti-Terrorism Act, 2015* (Ottawa: CBA, 2015).

no independent review at all[3], we support the creation of the NSIRA and its proposed responsibility for broad review of the national security infrastructure as a whole. We offer some suggestions for the wording and structure of sections of the proposed Act.

A. Mandate

The broadest portion of the agency's mandate is defined in section 8(1)(b) as any activity of a department that "relates to national security or intelligence". While we commend the decision to avoid language that would unnecessarily restrict the agency's mandate, an overly broad mandate could hinder the agency's ability to focus and assess its performance against its mandate.

'Intelligence' is a broad term that includes many departments whose activities are largely separate from national security issues, ranging from the Canada Revenue Agency to Fisheries and Oceans Canada. 'National security' is also problematic given multiple definitions in existing legislation, notably the *CSIS Act* and the *Security of Canada Information Sharing Act (SCISA)*. While this definition presumably includes departmental activities under both those Acts, it is unclear whether activities under other laws fall under the definition of national security. For example, the *Secure Air Travel Act (SATA)* does not refer to 'national security' and it is unclear whether review of *SATA* activities under that Act would be part of the mandate of the NSIRA.

RECOMMENDATION

1. **The CBA recommends that the mandate of the NSIRA be more explicitly articulated and precisely defined.**

Our comments on the definitions to establish the agency are:

(i) **Section 2, Definition of deputy head** – this seems to be replicate the definition of 'department head' in section 29 of the *CSIS Act*. It should also include the Chief of the Communications Security Establishment (CSE).

(ii) **Section 10, Right of access-complaints** – The words ''and of any other department'' should be added to each paragraph since other departments, such as the Department of National Defence, the Canadian Forces or Canada Border Services Agency, could be actively involved in matters being investigated.

---

[3] The CBA has expressed concerns about the lack of independent review of the CBSA in several past submissions. See *Privacy of Canadians at Airports and Borders* (Ottawa: CBA, 2017); *New National Immigration Detention Framework* (Ottawa: CBA, 2017), and *Our Security, Our Rights: National Security Green Paper, 2016* (Ottawa: CBA, 2016).

The Review Agency, consisting of a Chair and three to six members under section 3, has a mandate under section 8. However the role of the Chair is not defined, nor does it mention the Chair having direct control of resources to accomplish that role. Rather, Bill C-59 would give control of the resources necessary to fulfill the Agency's mandate to the executive director of the Secretariat, under sections 45 and 46. The Bill does not state that the executive director would report to the Chair of the Review Agency, but rather that the Secretariat is to "assist the Review Agency in fulfilling its mandate" (under section 41(2)). Presently the Chair of the Security Intelligence Review Committee is also the CEO of SIRC (*CSIS Act*, section 35), with control over the committee's resources under section 36.

In our view, the Chair of the NSIRA must control the agency's resources. The Intelligence Commissioner has been given that control under sections 5, 6 and 7 of the *Intelligence Commissioner Act*.

RECOMMENDATIONS

2. **The CBA recommends that the definition of 'deputy head' in section 2 be amended to include the Chief of the Communications Security Establishment.**

3. **The CBA recommends that the words ''and of any other department'' should be added to each subsection of section 10.**

4. **The CBA recommends that the Chair of the NSIRA control the Agency's resources.**

III. NATIONAL SECURITY AND PRIVILEGE

The proposed *NSIRA Act* would create a new agency with the mandate to review "any matter that relates to national security or intelligence" under section 8, but without defining 'national security' and 'intelligence'. The agency would have access to any information (other than a Cabinet confidence) that it 'deems necessary' to conduct its work (sections 9-11). This would extend to information subject to solicitor-client privilege, professional secrecy of advocates and notaries, or litigation privilege. In effect, the Act would create an open-ended mechanism to review the legal advice given to government.

The Supreme Court has commented that:

> The importance of solicitor-client privilege to our justice system cannot be overstated. It is a legal privilege concerned with the protection of a relationship that has a central importance to the legal system as a whole…
>
> Without the assurance of confidentiality, people cannot be expected to speak honestly and candidly with their lawyers, which compromises the quality of the legal advice they receive. […] It is therefore in the public interest to protect solicitor-client privilege.[4]

The privilege applies equally to government. The law draws no distinction amongst clients: principles of solicitor-client privilege apply with equal force to a government client as they do to a private client. It is critical for government to be able to obtain professional legal advice without the chilling effect of potential disclosure of its confidences. The quality of legal advice obtained by the federal government will inevitably be compromised if the confidentiality of its solicitor-client communications cannot be assured.

The Supreme Court has acknowledged that "certain government functions and activities require privacy. This applies to demands for access to information in government hands. Certain types of documents may remain exempt from disclosure because disclosure would impact the proper functioning of affected institutions".[5]

The CBA believes that there must be protection for records held by government that are subject to solicitor-client privilege. Recognition and protection of solicitor-client privilege promotes the public interest and the rule of law. Courts have long recognized that protecting the solicitor-client confidences of government promotes the public interest by enhancing application of the law and maintaining the rule of law over public administration.

> [...] the public interest is truly served by according legal professional privilege to communications brought into existence by a government department for the purpose of seeking or giving legal advice as to the nature, extent and the manner in which the powers, functions and duties of government officers are required to be exercised or performed. If the repository of a power does not know the nature or extent of the power or if he does not appreciate the legal restraints on the manner in which he is required to exercise it, there is a significant risk that a purported exercise of the power will miscarry. The same may be said of the performance of functions and duties. The public interest in minimizing that risk by encouraging resort to legal advice is greater, perhaps, than the public interest in minimizing the risk that individuals may act without proper

---

4 *Alberta (Information and Privacy Commissioner) v. University of Calgary*, [2016] 2 SCR 555, 2016 SCC 53 at para. 26, 34

5 Ontario (Public Safety and Security) v. Criminal Lawyers' Association, [2010] 1 SCR 815, 2010 SCC 23, at para. 40.

> appreciation of their legal rights and obligations. In the case of governments no less than in the case of individuals, legal professional privilege tends to enhance the application of the law, and the public has a substantial interest in the maintenance of the rule of law over public administration.[6]

It has been argued that privileged information must be made available because the practices of security agencies often depend on the legal advice they receive. However, without assurances of privilege, legal advice will be sought less often, will be based on less candid disclosure by clients, or worse, sought and received but not documented.

We strongly encourage reconsideration of the proposal to do away with privilege in matters of national security or intelligence. While the Bill does seek to protect disclosed information against claims of waiver and ensure that privileged information does not find its way into certain reports (section 53), we believe these miss the underlying rationale for protecting the privilege.

The Supreme Court has stated that the only way to preserve privilege is to ensure that it remains near absolute: "[a]bsolute necessity is as restrictive a test as may be formulated short of an absolute prohibition in every case". The Supreme Court has also stated that the privilege will "only yield in certain clearly defined circumstances."[7] These include:

- in the interests of public safety, where there are real concerns that an identifiable individual or group is in imminent danger of death or serious bodily harm;
- where an accused's innocence is at stake and access is necessary to allow the accused to make full answer and defence, or where "core issues going to the guilt of the accused are involved and there is a genuine risk of a wrongful conviction"; and
- to determine the validity of a trust agreement after the death of the settlor.[8]

The extremely limited nature of these exceptions "emphasizes, rather than dilutes, the paramountcy of the general rule"[9] of the near-absolute protection of the privilege.

The Supreme Court has mused about but not yet recognized an exception for national security. Professor Adam Dodek has cautioned that:

> The notion of what constitutes a threat to national security is highly subjective and history has shown that many abuses of civil liberties have occurred in this country and in others in the name of national security. [10]

---

6 *Waterford v. Australia* (1987), 163 C.L.R. 54 (H.C.A.) at p 74-75, as cited in *R. v. Ahmad* (2008), 2008 CanLii 27470 (Ont.S.C), 77 W.C.B. (2d) 804, 59 C.R. (6th) 308 (Ont.S.C.).

7 *R. v. McClure*, 2001 SCC 14.

8 *Ibid.*

9 *Ibid.*

10 Adam M. Dodek, *Solicitor-Client Privilege* (Markham: LexisNexis Canada Inc, 2014) at 276-277.

He goes on to argue that many of the situations where one might argue for a national security exception are already covered by the public safety exception.

We believe the case against a national security exception is even stronger in the circumstances of the Review Agency, which largely addresses *post facto* oversight.

Likewise, we do not believe the CSE or CSIS should be authorized to acquire privileged information other than in the clearly defined exceptional circumstances described above and subject to the requirement that there be minimal impairment of the privilege. Consequently, we recommend that Bill C-59 should not include open-ended access to all records, including those subject to solicitor-client privilege.

RECOMMENDATION

5. The CBA recommends that section 9(2) and (3) be removed from the NSIRA.

IV. INTELLIGENCE COMMISSIONER

The CBA supports the creation of an independent, specialized office for the oversight and authorization of activities by the CSE and CSIS. While we have generally called for judicial oversight, we recognize the advantages of a dedicated commissioner with staff and resources to allow for effective ongoing oversight. We offer suggestions about the structure of the position and related processes.

The CBA is concerned with the process of appointment of the Commissioner in section 4 of the proposed *Intelligence Commissioner Act*. Given the important oversight role to be played by the Commissioner, we suggest the appointment should be based on the recommendation of a Parliamentary Committee of all parties, or at least vetted by a Parliamentary Committee, rather than on the recommendation of the Prime Minister alone.

In considering the pool of candidates for the role of Intelligence Commissioner, the government should take special note of the expertise of retired judges of the Federal Courts in national security matters. The Federal Court and Federal Court of Appeal are defined as superior courts in the *Federal Courts Act*.

RECOMMENDATIONS

6. **The CBA recommends that the Intelligence Commissioner be appointed on recommendation of an all-party Parliamentary Committee, or at least that proposed appointments be vetted by a Parliamentary Committee.**

B. Reasonableness Review

The CBA is concerned about the nature of the review mandated by sections 14 to 21 of the proposed *Intelligence Commissioner Act*. The overall structure of the associated acts leads to nested findings on a reasonableness standard. For example, section 35 of the proposed *CSE Act* would allow the Minister to issue authorizations if there are 'reasonable grounds to believe' the relevant conditions are met. The Intelligence Commissioner would then review those conclusions for reasonableness under section 14 of the *Intelligence Commissioner Act*.

This raises two related concerns. The first is the implication of a nested reasonableness assessment. The structure of the mechanism suggests some deference to the Minister's initial opinion that a 'reasonable grounds' standard has been met. However, what it means for the Commissioner to find that the Minister's finding of 'reasonable grounds' is reasonable is unclear. Presumably, there would be cases where the Commissioner is not satisfied that there were reasonable grounds for that conclusion, but still finds the Minister's conclusion to fall in a range of reasonable outcomes. If that is true, the oversight mechanism proposed is commensurately weaker than it might appear. If not, there is no reason for the nested reasonableness assessments.

The second concern is connected to the first, and arises from the fact that courts in general are struggling with the application of the deferential standard of 'reasonableness review' in the administrative law context. There are ongoing debates about the level of deference implied by the reasonableness standard, and whether deference applies to interpretations of law. How these issues will be resolved is uncertain, as they arise from a fundamental tension between administrative decision-makers and the judicial review of administrative action. Framing the Commissioner's review in terms subject to this debate is unnecessary and would mean that the Commissioner's role could change as jurisprudence in the area of standards of review evolves.

These concerns could be addressed by framing the Commissioner's oversight as other applications for judicial authorization. Section 35 of the proposed *CSE Act* and associated sections of the proposed *Intelligence Commissioner Act* could be amended to require that the Minister may issue an authorization if the Intelligence Commissioner concludes there are

reasonable grounds to believe the relevant criteria have been met. The reasonable grounds standard is well established in many areas of law, stable and relatively well understood. Similar amendments should be considered for the *CSIS Act* and related provisions.

RECOMMENDATION

7. The CBA recommends that the Information Commissioner be responsible for directly making findings on reasonable grounds rather than reviewing findings by a Minister for reasonableness. Sections 14 to 21 of the *Intelligence Commissioner Act* should be amended accordingly, as well as associated sections of the *CSE Act* and the *CSIS Act*.

The CBA also questions the underlying rationale of certain distinctions in section 21 for the Commissioner's review of the reasonableness of conclusions under sections of the *CSIS Act* relating to datasets. Under section 21(2), dealing only with foreign datasets, the Commissioner has three choices in making a decision: to approve the authorization; not to approve the authorization; or to approve it with conditions. Section 21(1), dealing with the review of conclusions on all but foreign datasets, allows the Commissioner only two choices, to approve or not to approve. The Commissioner cannot approve with conditions for those datasets. We see no reason for this distinction and recommend that the Commissioner be able to approve with conditions in all circumstances.

RECOMMENDATION

8. The CBA recommends that section 21(1) of the *Intelligence Commissioner Act*, be amended to give the Intelligence Commissioner the option of approving any authorization with conditions.

V. COMMUNICATIONS SECURITY ESTABLISHMENT

Bill C-59 would enact the *Communications Security Establishment Act* (*CSE Act*) to replace and expand the current CSE authorities under the *National Defence Act* (*NDA*). The CBA supports the goals of greater clarity, transparency and oversight exhibited by the proposed legislation. The proposed *CSE Act* gives explicit authority for certain activities now only implicitly permitted under the *NDA*, and creates a regime of clear conditions and restrictions, including privacy protections, for the exercise of those authorities.

A. Oversight and Review

In addition to prior review of certain authorizations by the Intelligence Commissioner, Bill C-59 proposes that all CSE activities would be reviewed by the proposed NSIRA for lawfulness and to ensure that the CSE's activities are reasonable, necessary and comply with ministerial directions. The NSIRA would serve as the review body for complaints against the CSE.

The CBA supports the creation of the NSIRA and its review role. We also support the creation of the office of the Intelligence Commissioner and commend the government for integrating a mechanism for independent oversight and prior authorization for many of the most intrusive activities of the CSE. Our concerns about the framing of the Intelligence Commissioner's authorizations are outlined above and we make the following recommendation for the *CSE Act*.

RECOMMENDATION

9. The CBA recommends that section 35 of the *CSE Act* and associated sections of the *Intelligence Commissioner Act* be amended to require that the Minister may issue an authorization if the Intelligence Commissioner concludes there are reasonable grounds to believe the relevant criteria have been met.

Once an authorization has been approved by the Intelligence Commissioner, the Minister could extend the authorization without further review under proposed section 37(3). The length of an authorization could clearly be relevant to its reasonableness, so we believe the Intelligence Commissioner should review and authorize extensions to the period of validity.

RECOMMENDATION

10. The CBA recommends that section 37(3) be amended to require review by the Intelligence Commissioner.

B. Mandate

The CBA generally supports the more detailed mandate in the proposed *CSE Act*, which increases transparency and clarity for those working for the CSE and the public more generally. The *Act* outlines five activities for the CSE:

(i) foreign intelligence gathering
(ii) defensive foreign cyber operations
(iii) active (e.g. disruptive) foreign cyber operations

(iv) cybersecurity and information assurance for federal government institutions and other (i.e. non-governmental) organizations designated as being of importance to the government

(v) technical and operational assistance to federal law enforcement agencies, the Canadian Armed Forces and the Department of National Defence.

The current *NDA* expressly grants the CSE, authorities only for foreign intelligence gathering and protecting computer systems of the federal government. Apart from extending authority for cybersecurity and information assurance activities to non-governmental organizations under category (iv), it seems the CSE could conduct all the listed activities under the current *NDA*. Still, the clarity of the proposed list adds precision as to the scope of the mandate.

A challenge facing the CSE under the proposed mandate is that several elements are inherently in tension with each other. Offensive and defensive cyber operations have goals and practices that are fundamentally in tension, in particular in the context of disclosing cyber vulnerabilities the agency might discover. While there are compelling reasons for having the same agency address both offensive and defensive operations, given the overlapping nature of the underlying expertise and knowledge base, we suggest robust mechanisms to resolve this tension. The United States uses a formal Vulnerabilities Equities Process, and there are reports of a similar process for CSE, although details have not been made public.[11] If Parliament decides that the CSE mandate should continue to include both offensive and defensive cyber operations, a formal Vulnerabilities Equities Process should be implemented for Canada.

RECOMMENDATION

11. The CBA recommends that a clear and transparent Vulnerabilities Equities Process be part of the structure of the CSE if both offensive and defensive cyber operations remain part of its mandate.

In contrast to the activities of CSIS which may address both domestic and international security, the focus of the CSE is on activities of foreign entities and individuals. The *CSE Act* stipulates that foreign intelligence, defensive and active cyber operations and cybersecurity and information assurance activities may not be directed at any part of the global information infrastructure in Canada, or at Canadians or any person in Canada. However the Act acknowledges – and, apparently, expressly permits the CSE to collect personal information about Canadians or people in Canada, incidental to its activities related to foreign intelligence gathering and cybersecurity and information assurance operations. The *CSE Act* stipulates that

11 Report (http://bit.ly/2qYVdWy)

the CSE must take measures to protect the privacy of Canadians and people in Canada related to its use, analysis, retention and disclosure of personal information acquired in the course of the foreign intelligence and cybersecurity and information assurance aspects of the CSE's mandate. The Act does not expressly address privacy protective measures for any collection of personal information connected with defensive or active cyber operations. But the activities that may be carried out under these authorizations are broad and collecting personal information through those activities is clearly contemplated (e.g. "carrying out any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activities, authorized by the authorization"). Significantly, the Act seems to stipulate that no collection of personal information through those activities may be conducted except with authorization to conduct foreign intelligence or cybersecurity and information assurance operations. What is clear is that for an authorization to be issued, certain privacy protective conditions must exist.

The mandatory requirement for privacy protection measures is quite general, presumably anticipating that it will be further developed through appropriate policies and procedures. Still, there is no express requirement for policies or procedures to be adopted. Any authorization for the CSE to conduct cybersecurity and information assurance operations must specify the conditions or restrictions that the Minister considers advisable to protect the privacy of Canadians and people in Canada. The Governor in Council may make regulations about the privacy protection measures required to be adopted by the CSE, but there is no requirement to make those regulations.

The *CSE Act* permits *disclosure* of personal information obtained under the CSE's foreign intelligence or cybersecurity and information assurance operations, to people or classes of people designated by ministerial order if that disclosure is essential (foreign intelligence) or necessary (cybersecurity and information assurance) for the category of operations under which it was used or obtained. The CSE *may disclose* personal information without restriction to prevent the death or serious bodily harm of an individual.

The *CSE Act* requires that the CSE apply privacy protection measures to all its activities, but does not require those measures to be written, publicly available policies and procedures. The regulation-making authority in the *Act* permits the government to stipulate what the measures should provide. The CSE should develop and publish policies and procedures articulating the privacy protection measures it will apply in its operations, either through this regulation power or by ministerial direction.

RECOMMENDATION

12. The CBA recommends that the CSE develop and publish policies and procedures articulating the privacy protection measures it will apply in its operations, either through the regulation power or by ministerial direction.

C. Preamble

While the *CSE Act* largely pre-empts the *Privacy Act*'s application by granting express authority to collect personal information, *Charter* protections supersede that and apply to all CSE operations (in addition to the privacy protections in the *Act*.) While this overriding protection may be assumed, a preamble similar to that in the *CSIS Act* should be added to the *CSE Act*.

RECOMMENDATION

13. The CBA recommends that a preamble, similar to that in Bill C-59 for the *CSIS Act*, be added to the *CSE Act*.

D. Defensive or Active Cyber Operations

Authorizations for foreign intelligence and cybersecurity and information assurance operations must be approved by the Intelligence Commissioner to become effective. This approval is not required for defensive or active cyber operations, but a 'two-key' system of ministerial authorization must be followed. For defensive cyber operations, approval by the Minister of National Defence and consultation with the Minister of Foreign Affairs is required. For active cyber operations, approval by both Ministers is required. While no review and approval by the Intelligence Commissioner is stipulated for the CSE's defensive and active cyber operations and no specific privacy protection related to operations is stipulated in the *Act*, it appears to require that any collection of personal information connected with the operations be made pursuant to a foreign intelligence or cybersecurity and information assurance operation. It requires stipulated privacy protections and approval by the Commissioner. The CBA supports this requirement.

The *Act* allows general disclosure of information collected through CSE operations to people designated by the Minister, and that disclosure could include personal information. It may be made only if the information is essential for international affairs matters, including security and national defense (resulting from foreign intelligence gathering operations), or necessary for purposes of protecting information and cybersecurity infrastructures (resulting from

cybersecurity and information assurance operations). Consistent with a recent submission from the CBA on *SCISA*[12], we support the stipulation that disclosure must be 'required' or 'necessary', and not simply 'relevant' for those purposes. However, the guiding principles articulated in *SCISA* should also expressly apply to any sharing by the CSE:

(i) effective and responsible information sharing protects Canada and Canadians;

(ii) respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing;

(iii) entry into information sharing arrangements is appropriate when Government of Canada institutions share information regularly;

(iv) feedback on how shared information is used and whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information sharing;

(v) only those in an institution who exercise its jurisdiction or carry out its responsibilities in respect of activities directly related to the purpose of the sharing ought to receive information that is disclosed under the relevant legislation.

RECOMMENDATION

14. The CBA recommends that explicit reference be made in the *CSE Act* to the principles governing information sharing *SCISA.*

VI. CANADIAN SECURITY INTELLIGENCE SERVICE ACT

The CBA expressed serious concerns about introducing threat disruption powers to the *Canadian Security Intelligence Service Act* (*CSIS Act*) in Bill C-51, *Anti Terrorism Act, 2015*. [13] Bill C-59 would address many of those concerns, and we support proposed amendments to curtail those drastic powers.

Section 21.1(1.1) explicitly states what threat reduction measures may be taken, clarifying the scope of the activities envisaged. However, we remain concerned that the proposed kinetic powers move CSIS from the intelligence role it was designed to play. There were compelling reasons after events described in the *MacDonald Commission Report* to divide the intelligence gathering mandate of CSIS from the kinetic activities of other agencies. The move towards a kinetic mandate could alter the nature of CSIS and undermine the aims of its creation following the MacDonald Commission.

---

12 *supra*, note 3

13 *supra*, note 2.

We make a similar observation about the regime for unlawful conduct proposed in section 20.1. While the regime for unlawful conduct would be subject to review, oversight and increased transparency, the similarity of the regime to mechanisms in the *Criminal Code* only highlights the changing mandate and nature of CSIS.

Changes to sections 12.1(2) and (3) would clarify that any measures taken must comply with the *Canadian Charter of Rights and Freedoms*, addressing a primary concern we raised in previous submissions. However, section 12.1(3.2) still suggests that fundamental rights can be curtailed based on issuance of a warrant. Aside from authorizing searches under section 8 of the *Charter*, warrants cannot alter the constitutionality of state activities impinging on substantive *Charter* rights. If the proposed actions are a reasonable limit on *Charter* rights (other than those under section 8), judicial authorization is little more than a ruling to that effect. If this is in fact the intent of the proposed amendments, it should be clear.

RECOMMENDATION

15. The CBA recommends that proposed section 12.1(3.2) be deleted.

Sections 94 to 97 of Bill C-59 deal with operational and legal aspects of data collection, along with querying, exploitation and retention of data. Together these would create the new section 11.01 and subsequent sections of the *CSIS Act* addressing these matters.

These sections appear to respond to *In the Matter of an Application by XXX for Warrants Pursuant to Sections 12 and 21 of the CSIS Act*[14] (the Federal Court ruling). They are an amplified response that would create a new regime governing data processing by the CSIS.

In light of the Federal Court ruling, and the CBA's response to the federal government's Green Paper on National Security[15], we welcome the new regime and generally approve of the mechanisms proposed for implementation. However, further consideration must be given to the need for a dual administrative and judicial mechanism for data. Instead, the new regime should operate based on judicial authorization, keeping with the spirit of current sections 21 and 21.1 of the *CSIS Act.*

14 2016 FC 1105.

15 CBA Submission on *Our Security, Our Rights: National Security Green Paper, 2016* (Ottawa: CBA, 2016).

A. The Federal Court Ruling

The Federal Court ruling concerns the SIRC's 2014–2015 *Annual Report*, and involved an examination of CSIS use of metadata. The conclusion was that CSIS should have been more transparent[16] and the Court noted that it had not been informed of relevant practices by CSIS.[17]

The ruling is based on CSIS's use of data it collected as a *by-product* of the operation of warrants that authorized collection of information and communications under section 21 of the *CSIS Act*. It appeared that CSIS practice was that if information collected was related to a threat to the security of Canada[18], they could collect and retain both the informational content and the metadata associated with that content.[19] However, if the information collected was not threat-related, the content itself was destroyed while data related to the content were retained indefinitely.[20] The Court called this 'associated data'. The Court found retaining associated data was not authorized under the *CSIS Act* and was concerned by the breach of the duty of candour by CSIS. Only when the 2014-2015 SIRC report was published did the Court learn that CSIS had been unlawfully retaining associated data indefinitely since 2006.[21]

Also important in the ruling is the processing of metadata (specifically associated data) through modern analytical processes.[22] The data – including the datasets described in Bill C-59 – are unique in that at face value, they do not reveal any kind of threat. Sophisticated technical analysis may *deduce* information that may or may not be threat-related. Without that type of analysis, the data are only an apparently meaningless set of data about data. The Court notes:

> The ODAC is a powerful program which processes metadata resulting in a product imbued with a degree of insight otherwise impossible to glean from simply looking at granular numbers. The ODAC processes and analyses data such as (but not limited) to: [REDACTED]. The end product is intelligence which reveals specific, intimate details on the life and environment of the persons the CSIS investigates. The program is capable of drawing links

16 *Supra*, note 14 para. 14.

17 *Ibid*. para. 1. It is in this problematic context that the Court sat *en banc,* that is, with all designated judges concerned by this situation in attendance.

18 This concept is defined in section 2 of the *CSIS Act*.

19 *Supra*, note 14 at para. 34.

20 *Ibid*. at para. 33 and 34; see also para. 151.

21 *Ibid*. at para. 21: "The public *2014-2015 SIRC Annual Report* was tabled on January 28, 2016 in the House of Commons and made public the CSIS's retention of collected information through the operation of warrants. This was the first time I understood that the Service was indefinitely retaining third party information as a result of the operation of warrants."

22 *Ibid*. at para. 37.

> between various sources and enormous amounts of data that no human being would be capable of [REDACTED].[23]

The general legislative authorization in section 12 of the *CSIS Act* allows CSIS to collect, analyze and retain information related to threats to the security of Canada "to the extent that is strictly necessary", in what is generally referred to as CSIS's 'primary function'.[24] CSIS may apply to the Federal Court for a warrant to obtain, under section 21, judicial authorization to use intrusive methods of collecting information. Unlike section 12, the applicable standard is the reasonable grounds standard (rather than the reasonable suspicion standard). Both standards can exist harmoniously as a warrant is simply an additional tool that CSIS may require *in an ongoing investigation according to the parameters of its primary function*: this means that the requirements for reasonable suspicion, the existence of threat and the 'strictly necessary' standard continue to apply. Judicial control of CSIS's most intrusive activities is fundamental:

> [S]ection 21 was not enacted as a distinct and independent scheme from the primary function created by section 12(1). Rather, it was enacted to ensure rigorous procedural requirements and to provide a checks and balance system *through effective judicial control.*[25] (Emphasis ours)

The parameters of CSIS actions in its primary function to investigate threats to the security of Canada are important. Section 12(1) of the Act specifies that CSIS is legally authorized to collect, analyze and retain collected information and intelligence. The words "to the extent that it is strictly necessary" are after the clause saying they may collect this information and intelligence, but before the clause saying they may analyze and retain it.[26] The Attorney General's argument that the 'strictly necessary' standard applies to the collection of information only, not its analysis or retention, was based on this language.[27]

An essential finding in the ruling is precisely that the 'strictly necessary' standard should apply to the collection, analysis and retention of information, not just any of these parameters. This has significant repercussions for legislative amendments: data collected through warrants but

---

23 *Ibid*. para. 42.

24 *Ibid*. paras. 160, 161, 162. CSIS has 'secondary functions' set out in sections 13 (security assessments), 14 (advice to Ministers), 15 (ability to investigate) and 16 (assistance to the Ministers of National Defence or Foreign Affairs) of the *CSIS Act*.

25 *Ibid*. para. 172.

26 12(1): "The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada."

27 *Supra*, note 14, see Attorney General's position, para. 62.

unrelated to threats to the security of Canada cannot be retained by CSIS under the current Act.[28] The Court ultimately concluded that "the parameters set by section 12(1) do not permit the CSIS to retain non-target and non-threat information on a long-term basis. If the CSIS wants to retain such information not covered by its mandate, it must obtain the appropriate legislative changes to allow such retention."[29] Bill C-59 is an appropriate legislative response to the Court in the passage above.

B. Data Regime

Bill C-59 proposes new sections (beginning at section 11.01) that directly respond to the Federal Court ruling on metadata and associated data, specifically permitting CSIS to collect data not necessarily related to a threat to the security of Canada:

- collection and preliminary evaluation of information is essentially covered by an administrative framework, although part of the data may be obtained through warrants granted by the Court under section 21 of the Bill. In response to the Federal Court's observations, the judicial phase applies only to the *retention* of data on Canadians and persons in Canada. However, CSIS will be able to query and exploit datasets they are authorized by the Court to retain.
- some data (foreign datasets) are completely covered by an administrative framework.

We generally support different procedural and substantive mechanisms and safeguards, including those related to protecting privacy. However, we also support greater oversight by the courts for those administrative mechanisms.

Bill C-59 specifies that datasets[30] contain information that is personal but "does *not* directly and *immediately* relate to activities that represent a threat to the security of Canada". This echoes the Federal Court's definition of associated data (metadata not related to a target or threat), and adds clarity. The Minister may determine that a class of Canadian datasets:

> is authorized to be collected if the Minister concludes that the querying or exploitation of any dataset in the class *could lead* to results that are relevant to the performance of the Service's duties and functions set out under sections 12, 12.1 and 16 [subs. 11.03(2)].

---

28 *Ibid.* paras. 186, 187.

29 *Ibid*. para. 188.

30 A dataset is essentially a digital file with common characteristics (section 2).

The duties and functions referred to are the primary function of CSIS and one of its secondary functions. The French version reads:

> permettra de générer des résultats pertinents en ce qui a trait à l'exercice des fonctions qui lui sont conférées en vertu des articles 12, 12.1 et 16.

This differs in meaning from the English, creating *certainty* (permettra [will allow]) as to the generation of relevant results from Canadian datasets. If the oversight role of the Information Commissioner is to review for reasonableness, the French version is preferable.

RECOMMENDATION

16. The CBA recommends that the Minister's decision to approve a class of Canadian datasets for preliminary collection by CSIS be subject to a higher level of certainty if the intent is for the Intelligence Commissioner to only review the assessment for reasonableness.

Similarly, under section 11.05(1), CSIS must first be "satisfied that the dataset [it may collect] is *relevant* to the performance of its [primary and secondary] duties and functions". The relevance test reads slightly differently in the French: "*utile* dans l'exercice des fonctions". Again, this nuance could lead to diverging interpretations. The generally accepted French equivalent of "relevant" is "pertinent", rather than "utile".

RECOMMENDATION

17. The CBA recommends that the French and English versions of the Bill be reconciled to ensure consistent meaning.

Information that is *publicly available* "at the time of collection" [section 11.07(1)(a)] may be retained, queried and exploited [section 11.11(1)] without further formality, within or on expiry of the evaluation period (90 days) and if it is evaluated and confirmed as such.

The public nature of data raises another issue. Although the expectation of privacy generally diminishes or disappears when its object is in the public domain, inferences not obvious in the data themselves could still be obtained by processing the information through modern analysis methods, particularly when combined with other datasets. Those inferences could reveal information that would otherwise be subject to a significant expectation of privacy. What might the data—including publicly available data—reveal after being analyzed with powerful tools?

During the evaluation period and while CSIS is determining the class to which the data belong, CSIS shall not query or exploit these data. It may, however, consult them for specific purposes [sections 11.07(3) and (4)]. This is a key and consistent with the Federal Court's ruling.

Also during that period, CSIS may, among other things, apply "privacy protection techniques" [section 11.07(5)(d)]. The CBA supports applying techniques to protect the privacy of people whose data are being evaluated. The same applies to the possibility of deleting personal information not relevant to the performance of CSIS duties and functions and that may be deleted without affecting the integrity of the dataset [section 11.07(6)(a)].

CSIS is further limited under section 11.1(1). Paragraph (c) specifies that CSIS shall remove from a foreign dataset any information that relates to a Canadian or a person in Canada. Under paragraph (b), CSIS shall, in respect of a Canadian dataset, delete any information subject to solicitor-client privilege. Under paragraph (a), CSIS shall, in respect of a Canadian dataset or a foreign dataset, delete any information "in respect of which there is a reasonable expectation of privacy that relates to the physical or mental health of an individual". Although this expectation of privacy may go beyond physical or mental health, these are 'continuing' obligations on CSIS and they must be complied with during the evaluation period and beyond.

At the end of the 90-day evaluation period, if CSIS confirms that the data belong to the Canadian dataset class, it *shall* make an application for their retention to the Federal Court as soon as feasible, but no later than the 90th day of the evaluation period [section 11.09(1)]. If the data belong to the foreign dataset class, CSIS shall ensure that the dataset is brought to the attention of the Minister, again as soon as feasible but no later than the 90th day of the evaluation period, to enable their retention [section 11.09(2)]. If neither situation applies, CSIS shall destroy the data [section 11.09(3)].

The judicial stage of the procedure concerns data retention only. It is triggered by the Director (or a designated employee) after they obtain the Minister's approval (section 11.12). We support these administrative procedural measures, particularly obtaining the Minister's approval, being taken before an application for judicial authorization is made.

The judicial stage includes another standard of proof: the designated judge may authorize the retention of data if "the retention of the dataset that is the subject of the application is *likely* to assist the Service in the performance of its duties or functions under sections 12, 12.1 and 16" ("est *probable* que la conservation de l'ensemble de données […] aidera le Service") [section 11.13(1)(a)] (emphasis ours). This standard of proof should be *a minimum* for CSIS to retain—

and then to query and exploit—Canadian datasets during the authorized period, i.e., no more than two years. The same applies to the obligation for CSIS to comply with its continuing obligations under section 11.1 (deleting information that relates to physical or mental health, protecting client-solicitor privilege and removing information that relates to Canadians or persons in Canada from foreign datasets) [section 11.13(1)(b)].

Bill C-59 addresses several issues in the Federal Court ruling largely by moving away from the standard in section 12(1) of the *CSIS Act* that limits collection "to the extent that it is strictly necessary" to apply to the *collection, analysis* and *retention* of information gathered by CSIS during its investigation of activities that, based on reasonable suspicion, constitute a threat to national security. Bill C-59 substantially lowers the threshold for retaining Canadian datasets. Retention can be authorized if it is 'likely' to assist CSIS in the performance of its primary duties or functions, but the standard of 'likelihood' is less than 'strictly necessary'.

In our view, the standard of likelihood is insufficient to adequately protect the expectation of privacy for state retention of datasets related to Canadians or people in Canada. Would this aspect of the regime survive constitutional scrutiny under section 8 of the *Charter*, given the intrusive nature of the analytical processing of data and its ability to deeply affect privacy?

The procedural safeguards in the application include the obligation for CSIS to set out "any privacy concern which, in the opinion of the Director or the designated employee who makes the application, is exceptional or novel" [section 11.13(2)(d)]. Given this, the CBA supports this safeguard, also subject to terms and conditions imposed by the judge in the public interest [section 11.14(1)(e)]. The Bill confers a right of appeal on CSIS if the designated judge refuses to issue the requested judicial authorization [section 11.15(2)].

As mentioned above, once an authorization has been issued, CSIS may query and exploit the retained Canadian datasets. However, that querying and exploitation must *assist* CSIS in the performance of its primary duties and functions (sections 12 and 12.1) and must also be done "to the extent that it is strictly necessary" [section 11.12(2)]. This legal standard has been in section 12(1) since CSIS was created in 1984, and the Federal Court ruling is clear that it covers not only the collection, but also the analysis and retention of information gathered by CSIS.

The CBA believes it is appropriate for this standard also to cover the querying and exploitation of Canadian datasets. However, we again question whether the standard of being 'strictly necessary' should also apply to data retention as a condition for judicial authorization. We note that another standard, the "mesure nécessaire" in the French version ("extent that is

necessary"), is enough for the querying and exploitation of a Canadian dataset for the purposes of the Service's secondary function in section 16 of the Act.

The way the different standards are applied at different stages of dataset processing means it is not strictly necessary for CSIS to be able to retain the data, but their querying and exploitation must be strictly necessary. The risk of error in applying the 'strictly necessary' standard opens the door to a privacy breach since data retained by the state is subject to a lower standard.

On the same topic, the 'strictly necessary' standard applies to retention of the results of the querying or exploitation of a Canadian or foreign dataset "to *assist* the Service in the performance of its duties and functions under sections 12.1 and 15" [section 11.21(1)(b)] (section 12.1: measures to reduce threats; section 15: investigations for the purpose of providing security assessments and advice to Ministers). For the primary function (section 12), retention of results is not subject to a specific standard. For assisting the Ministers of National Defence or Foreign Affairs (section 16), retention of results is subject to the test of 'simple' necessity. The latter two situations reflect a legislative choice that indirectly fails to conform to the Federal Court's ruling, which applied a 'strict necessity' standard to information retention.

The proposed regime includes varying standards based on whether the activity is querying, exploitation, retention or the function or duty to be performed by CSIS. These subtle nuances, given the complexity of the proposed regime, could lead to debate and controversy, although the standards concerned are of no apparent operational relevance.

In the introduction, we questioned the need for Parliament to establish an administrative information collection regime (Canadian dataset classes approved by the Minister and subsequently by the Commissioner) instead of a system where a designated judge must approve the collection of information as part of the issuance of warrants. Again, this need is not obvious. Data collection is subject to an administrative regime, while the querying and exploitation of Canadian datasets are based on their retention (CSIS is prohibited from exploiting data during the evaluation period). The retention of Canadian datasets depends on judicial authorization. However, as the Court mentions in its ruling, these data are collected through the operation of warrants.[31]

It would be simpler to allow the designated judge to authorize CSIS to collect certain types of data as part of the warrants granted by the Federal Court under the current section 21. This would allow the designated judge to determine the legitimacy of the collection on a

31 Supra note 14, see excerpt from paragraphs 186 and 187 of the Court's ruling above.

case-by-case basis and according to the circumstances of each investigation leading to CSIS applying for a warrant. This would also apply to foreign datasets since CSIS may conduct investigations outside Canada [section 12(2)], including activities authorized in a warrant.[32]

RECOMMENDATION

18. The CBA recommends that retention of "associated data" be explicitly dealt with by the Federal Court judge authorizing a warrant when possible.

The administrative regime authorizing the collection of Canadian datasets following approval by the Intelligence Commissioner also raises the issue of judicial review of the Commissioner's decision in cases of refusal. For example, if CSIS determines, at the end of the evaluation period, that the collected data do not belong to an approved class, it may request a determination of a new class [section 11.08(4)]. If the Minister or the Commissioner refuses to approve the request for the determination of a new class, CSIS shall destroy the data. This raises the question of judicial review of the Commissioner's decision, or even the Minister's. This would also be an issue if exigent circumstances require the Commissioner to approve or refuse the decision by the Director of CSIS to authorize the query of a Canadian or foreign dataset not subject to a judicial or ministerial authorization. In that case, would the Commissioner's refusal be subject to judicial review? These questions are beyond the scope of this submission, but they would be largely moot in a regime where the designated judge had the duty of authorizing data collection on a case-by-case basis, with or without imposing terms and conditions in the public interest.

Foreign datasets may be retained with a ministerial authorization (section 11.17), based on the same standard of likelihood that applies to judicial authorizations.[33] CSIS must have complied with its continuing obligations (section 11.1). The Minister may, like the designated judge, impose terms and conditions in the public interest [section 11.17(2)(e)]. This approach seems appropriate given that a continuing obligations of CSIS is precisely to remove any information from foreign datasets that relates to a Canadian or a person in Canada [section 11.1(1)(c)]. The authorization is valid for five years [section 11.17(3)]. We support a distinction between the periods for Canadian and foreign datasets.

---

32 Section 12(3.1): "Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada."

33 Section 11.17(1)(b): "the retention of the dataset is likely to assist the Service in the performance of its duties and functions under sections 12, 12.1, 15 and 16".

Finally, the Minister shall notify the Commissioner of the Minister's determination of an authorization "for the purposes of the Commissioner's review and approval" (section 11.18). To echo our previous comment, the Bill provides for judicial review of the refusal by the Minister or Commissioner to approve the authorization to retain foreign datasets [sections 11.19(1) and (2)].

After authorization is granted, CSIS may query and exploit data subject of the ministerial authorization if "strictly necessary" [section 11.2(3)].

The scale and complexity of these provisions demonstrate Parliament's will to modify the data collection system to reflect technological progress and developments in case law, primarily the Federal Court ruling. We support these changes and adaptations.

The regime proposed is complex, and our comments about the terms and conditions are aimed at mitigating future disputes and promoting smooth application of the law, especially about the interaction between the administrative and judicial review mechanisms.

The regime requires a fine balance between national security requirements and the fundamental Canadian value of privacy, constitutionally enshrined in the *Charter*. The key question is to determine whether the balance in Bill C-59 meets constitutional standards.

VII. SECURITY OF CANADA INFORMATION DISCLOSURE ACT

The CBA has previously commented on the *Security of Canada Information Sharing Act* (SCISA), as it is now named – to be renamed the *Security of Canada Information Disclosure Act*. In January 2017, the CBA presented its submission on SCISA to the Access to Information, Privacy and Ethics Committee. We continue to have many of the concerns outlined there.

A. Definition of "activity that undermines the security of Canada"

We remain concerned with the breadth of the definition of "activity that undermines the security of Canada" in section 2, and also with the challenges of having different definitions of national security in different parts of Canadian law. Notably, the definition in section 2 of *SCISA* is substantially broader than the definition of "threats to the security of Canada" in section 2 of the *CSIS Act*.

Bill C-59 appears intended to restrict the definition of "activity that undermines the security of Canada" by varying the list of examples. However, the list is still not restrictive, introduced with the non-exclusive term "for greater certainty, it includes" which implies the definition is

broader than the list of examples. While the CBA welcomes more restrictive language surrounding some of the examples, the amendments do not clarify the intended scope of the *SCISA*. A clear, restrictive definition would give both clarity and transparency on a broad disclosure regime with substantial privacy implications.

The amendment to the exception in section 2(2) is troubling, as it substantially reduces the protection under the current version. In particular, a number of legitimate political activities might be seen on their face as undermining the "sovereignty" or "territorial integrity" of Canada. *Activities* among First Nations or Quebecois involving assertions of sovereignty, for example, should not, in and of themselves, trigger the disclosure provisions of the SCISA.

RECOMMENDATION

19. **The CBA recommends that the SCISA use the same definition of "threat to national security" as the CSIS Act. In the alternative, the definition of "activity that undermines the security of Canada" should be clearly restricted.**

20. **The CBA recommends that section 115(4) of Bill C-59 be deleted.**

The CBA supports the principles guiding information disclosure in section 4 of *SCISA*. However, to be effective, *SCISA* must include a robust oversight and accountability mechanism to enforce them. This mechanism should be independent from the government institutions that will be sharing or disclosing information. The proposed mandate for the *NSIRA* refers to the review of any activity that "relates to national security or intelligence", and so would presumptively include any information disclosure under *SCISA*. We expect that the mandate of the National Security Committee of Parliamentarians proposed under Bill C-22 would have a similarly broad application. As we have stated elsewhere, the CBA supports these review mechanisms and considers them to be a substantial improvement on the current situation.

In our January 2017 *SCISA* submission, the CBA also recommended that Schedule 3 list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statute supervised or implemented by those institutions that might relate to national security concerns. Several institutions in Schedule 3 have broad mandates that go well beyond national security. Despite the proposed amendments to section 5 of *SCISA*, there is still an implicit burden on disclosing institutions to be sufficiently familiar with a recipient institution's mandate to determine whether information will be relevant to the exercise of the recipient institution's jurisdiction or mandate. The CBA recommends guidelines for institutions

on what is actually needed, to prevent oversharing or over disclosure of information. The CBA also questions what obligations are imposed on receiving institutions to destroy information they receive that is not relevant.

The record keeping requirements in proposed section 9 do not require institutions to document how security interests are being weighed against privacy interests in the context of section 5(1) of *SCISA*. The CBA recommends that the statute include this information.

RECOMMENDATIONS

21. The CBA recommends that *SCISA* include effective mechanisms to enforce the principles in section 4.

22. The CBA recommends that Schedule 3 to *SCISA* be amended to list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes supervised or implemented by those institutions that may conceivably relate to national security concerns.

23. To prevent oversharing or over disclosure of information, the CBA recommends adopting guidelines for institutions on what is actually needed for the recipient institution to exercise its mandate. The CBA also recommends that *SCISA* address the obligations of recipient institutions if they receive information that is not relevant.

24. The CBA recommends that section 9 of *SCISA* include a requirement to document how security interests are being weighed against privacy interests, pursuant to section 5(1).

VIII. SECURE AIR TRAVEL ACT

Part VI of Bill C-59 proposes several amendments to the *Secure Air Travel Act (SATA)*. The CBA has expressed concerns over the practical functioning of secure air travel measures in the past,[34] as well as preclearance measures.[35]

---

34 CBA Submission on the *Anti-Terrorism Act*, 2015, *supra* note 2 and Green Paper, *supra* note 15, Submission on *Pre-Clearance Act* (Ottawa: CBA, 2016).

35 *Ibid*. *Pre-Clearance Act*, 2016.

The need for safe air travel must not be considered superordinate to *Charter* values or other Canadian rights and freedoms. Any measures toward that goal must be implemented in a clear, understandable and practical way so people and businesses (particularly airlines) affected know how to deal with rights and responsibilities. While the Bill offers some improvements to the current law, we remain concerned that it will do little to promote safe travel, negatively affect legitimate travel and commerce and provide questionable effective recourse for those harmed by its operation.

Revised section 6(2) would require an air carrier to give the Minister names, dates of birth and gender of an individual as well as any other information prescribed by regulation, if in the control of the air carrier. It is unclear what sort of information will be demanded of carriers or how this information would contribute to the safety of air travel. The current legislation requires that carriers provide information referred to in the schedule to the *Aeronautics Act*, a list of thirty-four items, but the actual changes to what must be provided under Bill C-59 are unclear. The regulation could allow demands for all that is listed in the *Aeronautics Act* schedule and more, with unknown scope for additional demands. It also seems that section 6(2) places no standard for the Minister to meet before demanding information from carriers. For example, the Minister need not have reasonable grounds to believe or even suspect that a person is engaged, or likely to engage, in acts detrimental to the security of air travel or criminal offences before demanding that information.

Further, the regulations may change without Parliamentary scrutiny. Air carriers may be required to provide a great deal of information about individuals, particularly if the regulation reflects the *Aeronautics Act* schedule. This could include information about the identity of travelling companions, prior flight information (from frequent flyer programs), credit card information on how tickets were purchased, business associations (where companies pay for employee or other travel) and so on. The contribution to safe air travel is unclear. It would be preferable for the legislation to list the information that could be demanded, and allow regulations to set only incidental, additional information as required.

In a free and democratic society, people have a right to go about their business undisturbed by state intervention. When one considers that the information collected could be shared with many entities (sections 10(b) to 10(f) includes the Minister of Citizenship and Immigration, the RCMP, CSIS, the CBSA and any other prescribed person or entity), a wide variety of information could be disseminated about any person. Under the proposed amendments to section 6 of the *SATA*, these entities and the Minister of Transport may demand information, not only about any

person who is a listed person, but also about anyone the entity has reason to believe is a listed person.

This casts a very wide net, to say the least. It raises the question of whether there are effective restrictions on the use these entities could make of the information or with whom it could be shared. The proposed section 6(6) requires the information to be used in the administration and enforcement of the *SATA*. This could cover virtually any possible use of the information if, for example, a police officer personally believes that the demanded information could be useful. The officer's reason to believe does not seem to be required to meet objective standards based on the drafting of the Bill. The legislation does not provide sufficient Parliamentary scrutiny of the information collected, sets a low bar for gathering information and does not appear to stop its wide dissemination. Considering how many have already been wrongly placed on no-fly lists, we recommend that at a minimum there be greater scrutiny of the type of information collected, the standard to be met before it is disseminated and protections against its misuse.

While there is a limitation in proposed section 6(6), on the ability of security agencies, including the RCMP, CSIS and CBSA, to demand information listed in the *Aeronautics Act* or prescribed by regulation (which may be interpreted broadly depending on future regulations), the limitation seems not to protect against intrusion. Information gathered may only be inferentially related to the administration and enforcement of the subject legislation and actually used to further other investigative actions. In our view, there is insufficient oversight for gathering information.

The information gathered under section 6(2) is not the same as the information that constitutes the no-fly list. It could affect many more people in many more ways. It has not been proven that this assists in promoting safe air travel and there is insufficient Parliamentary oversight of the type of information that could be demanded or how it could be used.

Section 8 of *SATA* permits a no-fly list to be established. No-fly lists are of questionable effectiveness and can be both over and under inclusive, and Bill C-59 does not address these issues. This is particularly true when the standard to place a person on the list is that the Minister has reasonable grounds to *suspect* that the person will engage in prohibited activities. Reasonable grounds to suspect is a low standard, and consideration should be given as to whether this is a sufficient basis for establishing a no-fly list, or whether the higher standard of reasonable grounds to believe is appropriate.

Bill C-59 adds some minor additional information about a person that can be included on a list, such as a middle name, but this is of questionable value. The section also permits potentially wide-ranging information about a person to be included if prescribed by regulation. This may perpetuate rather than attenuate the problem of over-inclusiveness. In our view, steps are needed to ensure that any information gathered by regulation serves to narrow those on this list and not interfere with the legitimate travel of Canadians and businesses. Similarly, the legislation should outline the sort of information that can be gathered by regulation with some specificity and narrow the category of information that can be gathered under this power.

The prior legislation suffered from an uncertain mechanism for removing names of innocent people from the no-fly list. Canadians are familiar with the story of a young boy on the list where his parents were unable to find out why or have him removed.[36] Section 15(6) proposes a deemed removal from the no-fly list and this is a welcome improvement over the deemed non-removal in the current Act. However, the time periods are unduly long. The Minister must make a decision within 120 days but may extend this a further 120 days. Eight months is a long time for a person to wait for removal from a list and could well interfere with legitimate business and personal travel. This may have many adverse economic and other effects and the time for removing a person from the list, or deemed removal, should be shortened.

The actual means of judicial review should also be improved. An affected party may seek to have the party's name taken off the no-fly list, but the Minister may require, with judicial approval, an *in camera* hearing. No authority is made to appoint a Special Advocate in these proceedings. Other national security matters permit a Special Advocate to protect the rights of the affected person, and we see no reason to deny this protection to people on the no-fly list.

It is vital that people have effective recourse to judicial review of any decision to deny their travel. Section 16(2) permits an appeal of a decision to place a person on the no-fly list and deny travel. We believe that the scope of review should not be limited to simple removal from a list. Where a person has been placed upon a list erroneously, the right to seek damages for that wrongful act must be recognized, at least if it is shown that the government was negligent in carrying out its statutory duties. Restricting the travel of Canadians in the name of safety must always be done in a professional manner based on proper information. The government cannot approach its statutory duties without regard for the interests of others. This raises the issue of

---

36 Parents of children hit by security problems urge independent no-fly-list system, on line (https://tgam.ca/2nabAKp)

how people wrongly placed on a no-fly list, having their personal or business travel disrupted, or even physical integrity compromised, should be compensated.

If the Minister does use the low standard of 'reasonable ground to suspect' to determine inclusion on the no-fly list, even given experience to date with the unreliability of lists and their questionable effectiveness, and their potential for interference with free travel and commerce, compensation should be available to innocent Canadians detrimentally impacted.

B. Review and Oversight

The review and oversight mechanisms that would apply to the *SATA* have not been made clear. Because the terminology of "national security" is not used in the Act, it is unclear whether activities under the *SATA* would fall into the mandate of the NSIRA, for example, and it is unclear what other review mechanisms would apply.

RECOMMENDATION

25. The CBA recommends clarity as to whether activities under the *SATA* would come under the review mandate of the *NSIRA* or some other review mechanism.

IX. CRIMINAL CODE AMENDMENTS

A. Listing Terrorist Entities

Given the significant implications of association with an entity listed under section 83.05, the CBA believes that the criteria on which the Minister decides to recommend listing an entity should be transparent, reviewable and regularly verified.

Bill C-59 makes a substantial change to the scope of criteria for listing under section 83.05 of the *Criminal Code*. It changes the relevant timeframe for entities under section 83.05(1)(b) that are currently acting on behalf of a listed entity to those who have historically acted in association with that entity. Given the historical nature of both sections, it is unclear how, once an entity was listed, it would ever be removed from the list. Entities such as the African National Congress, historically included on similar lists, may undergo substantial changes to become legitimate political parties. It is unclear how an entity would ever successfully challenge its continued listing under the current and proposed wording.

This concern also arises for the greater restrictions on reviews under section 83.05(2), which only allow review of historical evidence in relation to an entity, regardless of the passage of time. This seems incompatible with the new version of section 83.05(8), which appears to foresee the relevance of material changes in circumstances. Presumably the Minister would use other criteria to decide whether to recommend the continued listing of an entity, rather than simply looking at the historical record, or else there would be little need for review of the list. Those criteria should be made transparent and reviewable.

The CBA has a related concern with proposed section 83.05(8.1), which increases the period in which the Minister must review whether there are still reasonable grounds for an entity to be listed from two to five years. Given the significant implications and potential criminal sanctions facing any individual or entity associating with a listed entity, regular review is imperative.

The proposed section 83.05(10) increases to five years the period for publication of the results of the Minister's review in the *Canada Gazette*. This may be a drafting error, as there appears to be little reason for a five-year period prior to publication. In the interest of transparency, publication should continue to be required 'without delay'.

RECOMMENDATIONS

26. The CBA recommends that listing entities not be done solely on the basis of historical actions.

27. The CBA recommends that the listed entities continue to be reviewed every two years.

28. The CBA recommends that the drafting error in section 83.05(10) be fixed and require publication without delay.

B. Counselling Terrorism Offences

In 2015 and 2017, the CBA took the position that the section 83.221 "Advocating or Promoting Terrorism" offence is overbroad, vague and contrary to the core principle that the criminal law must be certain and definitive.[37] Further, the section requires only that the accused be reckless that a terrorism offence may be committed, and we believe that this low *mens rea* could be interpreted as a violation of section 7 of the *Charter*.

37 *Supra,* note 2.

The offence would now be restricted to individuals who counsel another person to commit a terrorist offence. Although the existing extensive case law for 'counselling an offence' could help in addressing these concerns, distinguishing terrorism offences from general counselling offences in the *Criminal Code* creates the possibility of disproportionate application, especially for people and groups that tend to be frequently associated with terrorism.

The changes appropriately address some constitutional concerns raised earlier by the CBA and others. Clause 143 of the Bill addresses many of the CBA's concerns by entirely replacing section 83.221. The proposed offence now consists of counselling another person to commit a terrorist offence. However, given that the offence of counselling already exists in the *Criminal Code*, we question whether the new offence would actually add further protection for Canadians. Duplicating existing offences unnecessarily increases the complexity the *Criminal Code* and could potentially lead to disparate lines of jurisprudence applying the same underlying principles.

RECOMMENDATION

29. The CBA recommends that section 83.221 be repealed.

C. Recognizances and Arrests

Prior to Bill C-51, the *Criminal Code* allowed peace officers to arrest and detain people on reasonable grounds to believe that a terrorist activity *will* be carried out and reasonable grounds to suspect that imposing a peace bond *is necessary* to prevent the terrorist activity. Bill C-51 replaced the requirement of a reasonable belief that "terrorist activity *will* be carried out" with a reasonable belief that terrorist activity "*may* be carried out". It also replaced the requirement that a recognizance or arrest of a person "is necessary to prevent the carrying out of the terrorist activity" with "*is likely* to prevent the carrying out of the terrorist activity."

In our view, the previous wording "will" and "necessary" combined with the requirement of "reasonable grounds to believe" and "proof on balance of probabilities" was adequate for judges to balance societal protection with individual liberty. Bill C-51 upset this balance and Bill C-59 should rectify this problem.

RECOMMENDATION

30. The CBA recommends that the wording in place prior to Bill C-51 be reinstated.

The CBA welcomes the repeal of sections 83.28 and 83.29, on investigative hearings and related arrests. The proposed amendments to section 83.3 are consistent with the CBA's recommendation that the previous thresholds for recognizances and related arrests – that were lowered in Bill C-51 – be restored.

X. YOUTH CRIMINAL JUSTICE ACT

The CBA supports proposed changes to the *Youth Criminal Justice Act* in Bill C-59. The amendments would help ensure that youth charged with terrorist-related offences, or subject to terrorist-related peace bond proceedings, would receive the enhanced procedural protections afforded under the *Act*. The proposed amendments safeguard and increase current protections. Inserting the phrase 'in a safe, fair and humane manner' in section 30(1) potentially gives additional protections to *all* young people who are detained, not just those involved in terrorist-related proceedings.

The rationale for amending section 119 of the *YCJA* to allow disclosure of youth records for the purposes of administering the *Passport Order* is unclear. On its face, this would appear to relate to the sections of the *Passport Order* allowing the denial of passport services in circumstances where an individual is subject to court imposed conditions not to leave the jurisdiction. If this is the rationale, the same concerns could be addressed by a limited query to the relevant authority administering youth sentences to verify whether a youth is permitted to leave the jurisdiction. Access to full youth records appears to be unnecessary.

XI. REVIEW

Section 168 of Bill C-59 mandates a comprehensive review of the provisions and operation of the Act "in the sixth year after the Bill comes into force" by Parliament: a committee of the Senate, the House of Commons or of both.[38] The committee would have one year to submit a report, including recommendations for change, but that one-year period could be extended by the parliamentary body.[39]

Comprehensive review of Bill C-59 would be aligned with the review of Bill C-22.[40] If the bills come into force within a year of each other, the required reviews could take place at the same

38 *Bill C-59*, s 168(1).

39 *Bill C-59*, s 168(2).

40 Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts*, 1st Sess, 42nd Parl, 2017 (assented to 22 June 2017), SC 2017, c 15, s 34.

time and by the same committee or committees.[41] Bill C-22 received Royal Assent on 22 June 2017 but is not yet in force, pending an order of the Governor in Council.[42]

A. Comments

The CBA generally supports the comprehensive review, with a few comments.

The review should be conducted by Parliamentarians, as proposed, as the importance of the matter calls for that minimum level of oversight. A Parliamentary body is the most suitable form – arguably the only one – to assess the operations of the Act and to recommend changes to ensure that measures to protect Canada's national security are consistent with the rule of law and the *Charter*.

We agree that the form of the committee to conduct the review should be left to Parliament and welcome the flexibility allowed for Parliament to extend the period beyond one year if needed to produce the report.

We also support the proposal that if the comprehensive review occurs within a year of the review of Bill C-22, it should be conducted by the same Parliamentary committee or committees. That approach takes advantage of committee members' expertise and experience. Although we appreciate that some period of operation is necessary before a comprehensive and meaningful review, it would help to understand the rationale for setting the mark at six years rather than aligning it with the five-year review of Bill C-22.

We also wonder why no subsequent reviews are provided. If an amendment to this effect is adopted, we suggest it be coupled with "…if an Act of Parliament amends this Act based on an independent review, the next report shall be tabled within six years after the day on which the amending Act is assented to".[43]

XII. IMPACT ON CHARITIES

Bill C-59 proposes few changes affecting charities and not-for-profits and their respective boards of directors. As explained in previous CBA submissions on national security issues, the interplay between existing laws and the broad audit and sanction capabilities of CRA have

41 *Bill C-59*, s 168(3), (4), (5).

42 *Bill C-22*, s 49.

43 See for example Bill C-15, *An Act to amend the National Defence Act and to make consequential amendments to other Acts*, 1st Sess, 42st Parl, 2013 (assented to 19 June 2013), SC 2017, c 24, cl 101, adding subs 273.601 (2) and (3) to the *National Defence Act*, RSC, 1985, c N-5.

resulted in significant problems for charities acting in conflict zones. They have impeded charities' ability to demonstrate effective control over charitable assets and programs to avoid placing the organizations and their directors, officers, employees and volunteers at risk.

Bill C-59 would amend the recently enacted *SCISA*[44] and rename it the *Security of Canada Information Disclosure Act*, emphasizing that the Act addresses only disclosure of information and not its collection or use. This is a positive step. Other amendments focus the definition of 'activity that undermines the security of Canada' and codify that advocacy, protest, dissent or artistic expression will not generally be considered to fall under 'an activity that undermines the security of Canada', narrowing the Act's application in a way the CBA supports. However, the Bill seems to also propose expanding its application by inserting the term 'threaten' into the definition.

The proposed *Criminal Code* amendments offer insight into the government's view of listed entities. While little would change procedurally, the focus of the Minister's role in making recommendations to the Governor in Council would change from recommending removal of a listed entity to recommending that the entity remain a listed entity. Further, the information considered on judicial review of the Minister's decision would be explicitly expanded to include information considered by the Minister in rendering the decision, and may still be heard in the absence of the entity or its legal counsel.

Bill C-59 proposes a mandatory review of the list every five years (or five years after an entity is added). This appears mainly a housekeeping measure, as it would have little effect on the organizations listed if they had not survived the listing process.

Section 83.221 of the *Criminal Code* would be replaced, changing the offence from 'advocating or promoting commission of terrorism offences' to 'counselling'. Similar to the broad facilitation offence in section 83.19, the new counselling offence would not require a terrorism offence to be committed or a specific terrorism offence to be counselled. While the term 'counsel' is not specifically defined, it would include 'procure, solicit or incite'. Like the facilitation offence, the new counselling offence could unduly expose charities and their boards to prosecution for charitable activities if they happen to be portrayed negatively.

---

44 S.C. 2015, c. 20, s. 2.

XIII. CONCLUSION

The CBA believes that Bill C-59 would make important improvements to national security law in Canada. We have highlighted several areas that still require some improvement, and look forward to working with the federal government to make the necessary changes.

SUMMARY OF RECOMMENDATIONS

1. **The CBA recommends that the mandate of the NSIRA be more explicitly articulated and precisely defined.**
2. **The CBA recommends that the definition of 'deputy head' in section 2 be amended to include the Chief of the Communications Security Establishment.**
3. **The CBA recommends that the words ''and of any other department'' should be added to each subsection of section 10.**
4. **The CBA recommends that the Chair of the NSIRA control the Agency's resources.**
5. **The CBA recommends that section 9(2) and (3) be removed from the NSIRA.**
6. **The CBA recommends that the Intelligence Commissioner be appointed on recommendation of an all-party Parliamentary Committee, or at least that proposed appointments be vetted by a Parliamentary Committee.**
7. **The CBA recommends that the Information Commissioner be responsible for directly making findings on reasonable grounds rather than reviewing findings by a Minister for reasonableness. Sections 14 to 21 of the *Intelligence Commissioner Act* should be amended accordingly, as well as associated sections of the *CSE Act* and the *CSIS Act*.**
8. **The CBA recommends that section 21(1) of the *Intelligence Commissioner Act*, be amended to give the Intelligence Commissioner the option of approving any authorization with conditions.**
9. **The CBA recommends that section 35 of the *CSE Act* and associated sections of the *Intelligence Commissioner Act* be amended to require that the Minister may issue an authorization if the Intelligence Commissioner concludes there are reasonable grounds to believe the relevant criteria have been met.**
10. **The CBA recommends that section 37(3) be amended to require review by the Intelligence Commissioner.**

11. The CBA recommends that a clear and transparent Vulnerabilities Equities Process be part of the structure of the CSE if both offensive and defensive cyber operations remain part of its mandate.

12. The CBA recommends that the CSE develop and publish policies and procedures articulating the privacy protection measures it will apply in its operations, either through the regulation power or by ministerial direction.

13. The CBA recommends that a preamble, similar to that in Bill C-59 for the *CSIS Act*, be added to the *CSE Act*.

14. The CBA recommends that explicit reference be made in the *CSE Act* to the principles governing information sharing *SCISA.*

15. The CBA recommends that proposed section 12.1(3.2) be deleted.

16. The CBA recommends that the Minister's decision to approve a class of Canadian datasets for preliminary collection by CSIS be subject to a higher level of certainty if the intent is for the Intelligence Commissioner to only review the assessment for reasonableness.

17. The CBA recommends that the French and English versions of the Bill be reconciled to ensure consistent meaning.

18. The CBA recommends that retention of "associated data" be explicitly dealt with by the Federal Court judge authorizing a warrant when possible.

19. The CBA recommends that the SCISA use the same definition of "threat to national security" as the CSIS Act. In the alternative, the definition of "activity that undermines the security of Canada" should be clearly restricted.

20. The CBA recommends that section 115(4) of Bill C-59 be deleted.

21. The CBA recommends that *SCISA* include effective mechanisms to enforce the principles in section 4.

22. The CBA recommends that Schedule 3 to *SCISA* be amended to list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes supervised or implemented

by those institutions that may conceivably relate to national security concerns.

23. **To prevent oversharing or over disclosure of information, the CBA recommends adopting guidelines for institutions on what is actually needed for the recipient institution to exercise its mandate. The CBA also recommends that *SCISA* address the obligations of recipient institutions if they receive information that is not relevant.**

24. **The CBA recommends that section 9 of *SCISA* include a requirement to document how security interests are being weighed against privacy interests, pursuant to section 5(1).**

25. **The CBA recommends clarity as to whether activities under the *SATA* would come under the review mandate of the *NSIRA* or some other review mechanism.**

26. **The CBA recommends that listing entities not be done solely on the basis of historical actions.**

27. **The CBA recommends that the listed entities continue to be reviewed every two years.**

28. **The CBA recommends that the drafting error in section 83.05(10) be fixed and require publication without delay.**

29. **The CBA recommends that section 83.221 be repealed.**

30. **The CBA recommends that the wording in place prior to Bill C-51 be reinstated.**