CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters*

Canadian Civil Liberties Association, January 2018

Table of Contents

Overview

Canadian Civil Liberties Association (CCLA)

The Canadian Civil Liberties Association (CCLA) is a national, non-profit, non-partisan and non-governmental organization supported by thousands of individuals and organizations from all walks of life. CCLA was constituted to promote respect for and observance of fundamental human rights and civil liberties and to defend and foster the recognition of those rights and liberties. CCLA's major objectives include the promotion and legal protection of individual freedom and dignity. For over 50 years, CCLA has worked to advance these goals, regularly appearing before legislative bodies and all levels of court.

Summary of Issues

As a defender of fundamental human rights and civil liberties, CCLA makes submissions to this Committee to express our serious concerns about several aspects of Bill C-59. While Bill C-59 makes some notable improvements to the Canadian national security landscape, it also fails to address a number of serious issues either created or exacerbated by the *Anti-terrorism Act, 2015*. Further, it introduces new provisions which may jeopardize or undermine the constitutional protections guaranteed in the *Canadian Charter of Rights and Freedoms*.

In our view, many aspects of Bill C-59 require substantial amendments—in order to both withstand constitutional scrutiny and adequately protect the rights and security of all persons in Canada. The bill is the most comprehensive attempt to modernize Canadian national security law in the last thirty years. Failing to resolve long standing critical issues is an opportunity Canada cannot afford to miss.

The new proposed *National Security and Intelligence Review Agency Act* and the *Intelligence Commissioner Act* both aim to create new accountability measures to provide review and oversight of agencies involved in national security. Our recommendations aim to strengthen these new bodies and address significant gaps in the proposed framework.

The proposed *Communications Security Establishment Act*—a new enabling statute for CSE—is welcome. Our recommendations focus on concerns about the new active cyber operations aspect of CSE's mandate, the expansive definition of "publicly available information," and gaps in relation to oversight and reporting of CSE's activities.

Bill C-59 maintains the threat reduction powers in the *Canadian Security Intelligence Service Act,* while also creating a new dataset regime for CSIS. Our recommendations aim to ensure that datasets are collected in relation to CSIS's mandate and that adequate record-keeping and accountability mechanisms exist. CCLA continues to question whether the necessity of threat reduction powers has been demonstrated but recognizes improvements made to the scheme first established by Bill C-51.

Bill C-59 proposes some substantial amendments to the controversial *Security of Canada Information Sharing Act (SCISA)*, but these fall short of repairing the issues identified when Bill C-51 was introduced and in subsequent study. Our recommendations propose changes to the trigger for disclosure and the thresholds for disclosure and retention. We also address gaps in accountability measures and the need for clarity regarding *SCISA*'s interaction with the *Privacy Act*.

The significant procedural failings of the *Secure Air Travel Act*, which can have devastating impacts on the lives of innocent individuals, have not been adequately rectified. Our recommendations would raise the threshold for listing and improve the appeal framework available to those who wish to challenge their listed status.

In relation to the *Criminal Code* amendments, we make recommendations on issues ranging from the terrorist entities list, to the terrorist speech and propaganda provisions to the peace bond and warrantless arrest provisions. In each instance, our concern is ensuring that the criminal law is deployed in a manner that prevents terrorist threats, while respecting fundamental *Charter* rights.

Finally, since the Committee may propose amendments outside the current scope of the bill, we recommend that the amendments made to the *Immigration and Refugee Protection Act* by Bill C-51 should be repealed. Those changes call the constitutionality of the security certificate scheme into question despite years of litigation preceding them. In our view, this Committee should amend Bill C-59 to address this issue.

The *National Security and Intelligence Review Agency Act*

The CCLA and others in civil society and academia have been advocating for the creation of an integrated agency that can review the national security activities of a number of agencies and departments for many years. In response, the government has proposed the creation of the National Security and Intelligence Review Agency. Our current recommendations seek to strengthen this agency in order to ensure that it can carry out its broad mandate, which includes responsibilities to review a wide variety of activities and investigate complaints. In our view, the relatively small number of members of the agency, and the decision to have the Chair and Vice-Chair serve as either full-time or part-time appointments, and all other members serve on a part-time basis, is not supported based on the nature and breadth of the agency's mandate. The size of the agency should be increased and/or the appointments should be full-time.

> **Recommendation 1:** Amend subsection 4(7) of the *NSIRA Act* so that all members of the NSIRA hold office on a full-time basis in recognition of the significant volume of work they are expected to carry out. In the alternative, if part-time status is maintained, the number of NSIRA members should be increased to a minimum of six, plus a full-time Chair.

We also propose adding some detail to the legislative language describing NSIRA's activities for the purposes of increased transparency. Currently, section 8 of the proposed *NSIRA Act* sets out the mandate of the review agency in broad terms, and the public reporting requirements are stated quite generally. When compared to the functions of the SIRC as currently set out in section 38 of the *CSIS Act*, the new provisions lack significant detail and seem to leave more to the new agency's discretion. Our proposals seek to ensure that the creation of a new review agency does not result in a loss of any review functions.

> **Recommendation 2:** Amend the *NSIRA Act* to clarify that NSIRA is explicitly responsible for performing the same functions with respect to CSIS as is currently done by SIRC.
>
> **Recommendation 3:** Amend the *NSIRA Act* to ensure that NSIRA is required to report publicly on the number of warrants issued under section 21.1 of the *CSIS Act* and the number of requests that were refused.[1]
>
> **Recommendation 4:** Amend sections 38-40 of the *NSIRA Act* to include language that clarifies that the reports that are made public should include *all* activities of NSIRA and unclassified versions of *all* findings and recommendations made by the Agency.
>
> **Recommendation 5:** Amend the *NSIRA Act* so that NSIRA is responsible for reviewing, on a regular basis, the structure and information provided by the CSE in its annual report and is explicitly authorized to recommend the CSE include specific information in future reporting, including periodic inclusion of statistical information regarding the nature and scope of its activities.[2]

The *Intelligence Commissioner Act*

The creation of a new office known as the Intelligence Commissioner appears to be aimed at providing real-time oversight and control in relation to some of the functions of CSE and some CSIS powers that are not currently subject to oversight by the Federal Court. With respect to CSE, some of its activities are currently reviewed by the CSE Commissioner.

---

[1] SIRC is currently required to do this pursuant to s. 53(2) of the *CSIS Act.* See also SECU's recommendations: House of Commons. Standing Committee on Public Safety and National Security. *Protecting Canadians and their Rights: A New Road Map for Canada's National Security.* 42nd Parliament, 1st Session (May 2017) [SECU, *Protecting Canadians and their Rights*].

[2] Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson and Ronald Deibert, *Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017)*, The Citizen Lab and the Canadian Internet Policy and Public Interest Clinic, Recommendation 53, online: https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf ("Citizen Lab/CIPPIC Analysis").

However, he or she has a narrow mandate to report on CSE compliance with the law and, in doing so, currently relies on CSE's own interpretations of the law. Independent oversight is of vital importance to ensuring that our security services act within the bounds of the law, including the *Charter*, and may help facilitate public confidence in their activities. Unfortunately, the regime established by Bill C-59 contains significant gaps that should be addressed to achieve these worthy goals. In particular, since the position of Commissioner has been described as "quasi-judicial", issues of tenure and compensation should be addressed to ensure it is truly independent and empowered to act judicially.

> **Recommendation 6:** Amend subsection 4(4) of the *Intelligence Commissioner Act* to set the remuneration of the Intelligence Commissioner in relation to the salary of a judge of the Federal Court, pro-rated to account for the fact that the position is part-time.

> **Recommendation 7:** Remove subsection 4(2) of the *Intelligence Commissioner Act* so that the Intelligence Commissioner may only serve a single, non-renewable term. In this case, the term set out in subsection 4(1) should be made longer than five years.

In the proposed *CSE Act*, the Intelligence Commissioner provides an oversight function for CSE foreign intelligence and cybersecurity authorizations issued by the Minister. The government has suggested that Intelligence Commissioner approval is not required for active and defensive cyber operations authorizations because—while some *Charter* rights may be engaged by activities authorized under these provisions—the acquisition of a Canadian's or person in Canada's private information would not be authorized.[3] This assumes that Intelligence Commissioner approvals should only be required on the basis of concerns about individual privacy. CCLA rejects this assumption. Activities under these authorizations will be carried out in secret and may well have significant impacts on the rights and legitimate expectations of Canadians and persons in Canada in ways they will likely never know. They may also have far-reaching impacts on internationally protected human rights and global security interests more broadly. While it is not our position that every activity conducted subject to an active or defensive cyber operations authorization will necessarily impact a *Charter* right in a manner requiring judicial authorization, some form of independent and impartial oversight is appropriate to ensure that these powers are exercised lawfully and with adequate restraint. Given the far-reaching implications of these powers, after-the-fact review by NSIRA is insufficient.

With respect to CSIS, the Intelligence Commissioner can authorize the initial collection of classes of Canadian datasets, the retention of foreign datasets, and classes of acts or omissions that certain CSIS employees may commit that would otherwise constitute

[3] Department of Justice, Charter Statement - Bill C-59: *An Act respecting national security matters* (Tabled in the House of Commons, June 20, 2017), <http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html>.

offences. In addition, the Intelligence Commissioner provides an after-the-fact review function in relation to CSIS queries of datasets in exigent circumstances to assess whether the basis on which the query was authorized was reasonable. However, it is unclear what consequence would flow from a determination that the query was not authorized.

Our national security agencies operate largely in secret, and while independent oversight may help to provide a check on the power of these agencies, there is likely to be little impact on public confidence if the oversight process consists solely of a closed dialogue between the relevant security agency and the Intelligence Commissioner, and if the outcomes of the approval process are also shrouded in secrecy. A more robust process is required to ensure that the Intelligence Commissioner hears not only from the security service seeking approval, but also from an individual or organization appointed to represent the public's interest in transparency and ensuring our national security agencies comply with the *Charter*.

Recommendation 8: Amend the *CSE Act* and the *Intelligence Commissioner Act* to require Intelligence Commissioner approval of active and defensive cyber operation authorizations granted by the Minister pursuant to sections 30 and 31 of the *CSE Act*.

Recommendation 9: Amend the *Intelligence Commissioner Act* to require the involvement of a special advocate, amicus, or similar entity to provide the Intelligence Commissioner with submissions in relation to the criteria for authorizations, amendments and determinations. This individual should be an independent, security-cleared lawyer with full access to all relevant information and evidence.

Recommendation 10: Amend paragraph 21(1)(a) of the *Intelligence Commissioner Act* to require that the Intelligence Commissioner issue reasons even in circumstances where an approval is granted and allow for the reasons and order to be made public, to the fullest extent possible.

Recommendation 11: Amend the *Intelligence Commissioner Act*, the *CSIS Act*, and the *CSE Act* to create bilateral appeal rights to the Federal Court (applicable to the security service and the special advocate or similar entity) in respect of an approval or a refusal to approve an authorization by the Intelligence Commissioner.

Recommendation 12: Amend the *Intelligence Commissioner Act* to expand the range of options available to the Intelligence

Commissioner by allowing him/her to attach conditions to authorizations in all cases.

The *Communications Security Establishment Act*

Bill C-59 creates for the first time a separate enabling statute for Canada's signals intelligence and cybersecurity agency, the Communications Security Establishment (CSE). The *CSE Act* is complex, and it is difficult to fully assess how much of the proposed legislation represents an attempt to place current and ongoing CSE operations into a public statutory framework, and how much of it affords the Establishment new powers. Whether the activities authorized by the *CSE Act* are existing or new, however, there is a great deal receiving public scrutiny for the first time, and CCLA has numerous concerns and recommendations in relation to the Act as a consequence. Our recommendations address:

- The addition of active and defensive cyber operations to the CSE's mandate
- The overbroad definition of publicly available information, combined with the lack of appropriate safeguards against misuse of such information
- Necessary improvements to oversight and reporting activities for CSE.

Active and Defensive Cyber Operations

Section 16 (2) of the *CSE Act* adds two aspects to CSE's mandate, "defensive" and "active" cyber operations. The "active" cyber operations aspect of the mandate expands the scope of CSE powers to include offensive hacking.

While active or defensive cyber operations are not to be "directed" at Canadians or persons in Canada,[4] or at any portion of the global information infrastructure in Canada,[5] this is an insufficient safeguard to prevent impacts on the rights and legitimate expectations of Canadians and people in Canada, none of whom can live their online lives exclusively within our national borders.[6] Not only do the privacy measures in place for other aspects of the CSE's mandate not apply to active or defensive cyber operations, but the *CSE Act* fails to acknowledge that these types of activities (e.g. undermining an encrypted messaging service, or altering content on a website) may have serious, albeit incidental, impacts on *Charter*-protected rights including freedom of expression, freedom of assembly, freedom of mobility, and potentially others, within Canadian borders. There is also no acknowledgment of Canada's obligation under international law to exercise some degree of respect for the privacy rights of foreign nationals.[7]

---

[4] Proposed (C-59) *Communications Security Establishment Act*, s. 23 (1).
[5] Proposed (C-59) *Communications Security Establishment Act*, s. 23 (2)(a).
[6] Indeed, research has demonstrated that even activities entirely conducted within Canada may result in information crossing borders: an email sent from an office at the University of Toronto to another office across the street on the same campus may well route through the United States on its way to its destination. See Andrew Clement and Jonathan Obar, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges," Chapter 1 in Michael Geist (ed), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, University of Ottawa Press, 2015 <https://ruor.uottawa.ca/bitstream/10393/32424/1/9780776621838_WEB.pdf>.
[7] International instruments identifying privacy as a human right, to which Canada is a signatory, include the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*.

These deficits are exacerbated by the absence of Intelligence Commissioner review of authorizations under these two aspects of CSE's mandate, leaving a notable accountability gap for these activities which will take place without external independent scrutiny. In the case of CSIS's threat reduction powers, which are in some ways analogous to these new aspects of CSE's mandate, the government has set out a complex framework for prior judicial authorization and a longer list of prohibited activities. While we do not concede the adequacy of that framework, it is notable that, in contrast, CSE's cyber operations activities involve no meaningful privacy protections, require only secret Ministerial authorization, and involve only after-the-fact review.

CCLA also shares the concern, expressed in detail in the December 2017 joint Citizen Lab/CIPPIC Analysis of Bill C-59, that putting the competing responsibility for defending Canada against security vulnerabilities while at the same time incentivizing the use of such vulnerabilities under an "active" mandate increases the tensions inherent to the CSE's multi-faceted mandate, and provides inadequate statutory direction to assist in establishing priorities or managing risks.[8]

> **Recommendation 13:** Do not adopt the provisions in the *CSE Act* related to active cyber operations, and refer the issue for further study to evaluate the necessity and proportionality of these powers.
>
> **Recommendation 14:** In the event that it is deemed to be necessary and proportionate based on a compelling and publicly defensible rationale, appropriate guidance should be included in the *CSE Act* to ensure that there are statutory safeguards in place to address situations when priorities within defensive and active cyber operation mandates conflict.
>
> **Recommendation 15:** Amend section 25 of the *CSE Act* to include defensive and active cyber operations as activities also requiring measures to protect privacy.
>
> **Recommendation 16:** Amend section 61 (b) of the *CSE Act* to require consultation with the Privacy Commissioner of Canada when making or revising regulations respecting the measures referred to in section 25 to protect privacy.

Publicly Available Information

While the majority of CSE activities cannot be directed at Canadians or persons in Canada as per section 23(1), section 24 creates an exception for "publicly available information," defined in unacceptably broad terms, as information accessible on the global information

[8] See Citizen Lab/CIPPIC Analysis at 62-68.

infrastructure *or otherwise*, or that is available on request, by subscription, or by purchase.[9] This permits a vast amount of information, including from within Canada, and/or created by or about Canadians or persons in Canada, to be collected in bulk. There are no privacy protections for its acquisition or collection, and privacy protections for use, analysis, retention and disclosure are left to regulation, the terms of which are typically subject to less public scrutiny or debate than legislation.[10] Furthermore, nothing precludes the acquisition of illegally obtained materials, which raises the risk of creating incentives for the acquisition and provision of questionably-obtained information, including grey and black market information from hacks and breaches, to CSE. There is also no external oversight of such collection to ensure it is firmly linked to the Establishment's mandate, as the Intelligence Commissioner has no role in relation to publicly available information.

The breadth of the proposed definition can be contrasted with another law that creates exceptions for publicly available information: Canada's private sector privacy law. The *Personal Information and Protection of Electronic Documents Act* (PIPEDA) allows companies to use publicly available information without obtaining individual consent, but the relevant regulation defines publicly available information narrowly by specifying five categories of information that are public for the purposes of the Act.[11] Canada's other private sector privacy laws have similar, closed lists of information types considered public. The definition in the *CSE Act*, in contrast, would allow almost unfettered access to personal information online, a scope that has not been demonstrated to be necessary, even in submissions by the CSE on this Act, and which is clearly disproportionate to the needs which have been expressed publicly.[12]

Presumably, the restriction regarding directing activities at Canadians or persons in Canada that guides most CSE activities has been lifted in relation to "public" information in this bill because of an underlying assumption that no privacy interests adhere to such information. That assumption is false. It is simply not true that there is never a reasonable expectation of privacy in information that individuals make public online, or that is public by virtue of the way digital communication technologies or platforms are designed and function. Canadian courts have affirmed that electronic conversations deserve privacy protection under s. 8 of the *Charter*;[13] that anonymity online deserves protection,[14] and that publicly available

[9] Proposed (C-59) *Communications Security Establishment Act*, s. 2.
[10] Proposed (C-59) *Communications Security Establishment Act*, s. 25.
[11] This includes phone book information, business directory information, information in a registry collected under statutory authority, information in records of a judicial or quasi-judicial body, and information in a publication in printed or electronic form, if an individual provided it. In most cases, the overriding principle is that uses of such public information should still be consistent with the purpose for which it was collected.
[12] For example, Mr. Dominic Rochon, Deputy Chief, Policy and Communications, CSE, in response to a question from Member of Parliament Mr. Matthew Dubé, identified the need to access public information explaining "exactly how the global information infrastructure is actually set up" as a rationale for accessing publicly available information. Such information could be addressed by the ability to subscribe to public reports and academic or technical journals. Evidence, Thursday November 30, at 10:45 <http://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-88/evidence>.
[13] Most recently *R v Marakah*, 2017 SCC 59; *R v Jones*, 2017 SCC 60.
[14] *R v Spencer*, 2014 SCC 43 [*Spencer*].

information is not disqualified from being personal information simply because it is public.[15] The definition of "publicly available" should not be so broad as to include information in which Canadians or people in Canada may arguably retain privacy interests. This provision, in other words, must not be a loophole through which CSE can acquire (and potentially, as per section 24(1)(a) disclose) information about Canadians or people in Canada which would otherwise be inaccessible to them by law. Further, it should be explicit that the Privacy Commissioner of Canada has the right, as per s. 37(1) of the *Privacy Act,* to investigate to ensure compliance with sections 4-8 of that Act in relation to CSE use of publicly available personal information.

Recommendation 17: Amend the definition of "publicly available information" in section 2 of the *CSE Act* to:

a) specify that it only includes information that has been published or broadcast for public consumption without restriction;
b) remove the term "otherwise";
c) Limit the ability to purchase or subscribe to information from the definition, to specify that information for which remuneration is provided must be legally available to the general public, and that was legally obtained or created by the vendor (i.e. limit the purchase of information to "commercially available publications and broadcasts"[16]).

Recommendation 18: Amend section 24 of the *CSE Act* to add a limit to the activities listed in 24(1) namely: The measures shall be reasonable and proportional in the circumstances, having regard to the reasonably foreseeable effects on Canadians and people in Canada including on their right to privacy.[17]

Recommendation 19: Amend the *CSE Act* to specify that publicly available information that identifies or is linked to an identifiable Canadian or person in Canada may only be disclosed if it is deemed essential to defence or security. Any such disclosures should be subject to independent review by NSIRA to ensure they meet that threshold.

[15] Teresa Scassa, "Privacy and Publicly Available Personal Information, 11 Can. J.L. & Tech. 1, 2013. at 3; *UFCW-Can, Local 401 v Alberta (Information and Privacy Commissioner)*, 2012 ABCA 130.
[16] This wording is from the Citizen Lab/CIPPIC Analysis, see Recommendation 40, at 54.
[17] The concept of imposing such a limit and the wording suggested are modeled on the *CSIS Act* section 12(2) as amended in Bill C-59.

Oversight and Review

CCLA supports the oversight role that the Intelligence Commissioner has been positioned to play in relation to previously unexamined Ministerial authorizations. Similarly, we are encouraged that longstanding calls to provide integrated review of Canada's national security and intelligence agencies have been answered with the proposed creation of the National Security and Intelligence Review Agency. It is essential that the powers granted to those bodies are sufficiently rigorous for them to fulfil their potential as a made in Canada, state-of-the-art response to the need for effective, rights-respecting national security operations. We also suggest that greater public reporting requirements would help to improve the transparency of CSE's activities.

These recommendations must be read in conjunction with those CCLA recommends in relation to the *Intelligence Commissioner Act* and the *National Security and Intelligence Review Agency Act* (*NSIRA Act*).

> **Recommendation 20:** Require Intelligence Commissioner approval in addition to current provisions for Ministerial authorization and the approval and/or informing of the Minister of Foreign Affairs for all active and defensive cyber operations.
>
> **Recommendation 21:** Require Intelligence Commissioner approval of authorizations issued under sections 30 and 31 of the *CSE Act* in addition to the current reporting requirements to NSIRA mandated in s. 53.
>
> **Recommendation 22:** Amend section 60 of the *CSE Act* to require CSE to include in its annual report how frequently active and defensive cyber operations are carried out.[18]
>
> **Recommendation 23:** Amend section 60 of the *CSE Act* to require CSE to include in its annual report the frequency at which it provides technical and operational assistance to other entities, and which agencies receive that assistance.[19]

Canadian Security Intelligence Service Act Amendments

There are two main issues addressed in the amendments proposed to the *CSIS Act* that CCLA will address: a process for the use of datasets by CSIS and refinements to the threat reduction powers introduced in Bill C-51. Each of these is addressed below.

[18] This recommendation is similar to Recommendation 54 in the Citizen Lab/CIPPIC Analysis.
[19] This recommendation is similar to Recommendation 52 in the Citizen Lab/CIPPIC Analysis.

The New Dataset Regime

The new dataset regime set out in the proposed amendments is designed in part to address the Federal Court's 2016 decision in *Re X,*[20] which determined that CSIS had been retaining certain information in the absence of a clear authority to do so, and had failed in its duty of candour to the Court in seeking approvals for certain warrants. The Service had obtained non-threat related information from intelligence gathered through warrants, including information about individuals who were not the targets of surveillance. The Federal Court held that CSIS had no authority to retain information that was unrelated to a threat to the security of Canada. Despite some acknowledgement in the decision that querying and exploitation of some of the information improperly retained had proven useful to the Service, the Court found that it was not authorized by law. The regime set out at proposed ss. 11.01 - 11.25 responds to the decision and takes the collection of datasets generally outside of the judicial authorization scheme, with different protections set out for different activities in relation to the datasets.

The regime applies to datasets that contain personal information and that *do not* directly and immediately relate to activities that represent a threat to the security of Canada. For Canadian datasets, the Minister can authorize collection of a class of datasets if the Minister concludes that querying and exploitation of *any* dataset in the class *could* lead to results that are *relevant* to the performance of the Service's intelligence, threat reduction or foreign intelligence roles. This is a low bar and does not define which datasets, if any, are clearly off the table. However, the collection of publicly available datasets and foreign datasets is not even constrained in this manner.

There is no meaningful definition of "publicly available dataset". It is defined in a manner that is circular and tautological. If it is interpreted in line with the definition of publicly available information in the *CSE Act*, the same concerns expressed above at pages 8-10 apply.

Further, while there are significant record-keeping requirements in relation to all types of datasets, these requirements are carried out by CSIS and very few of them extend outside the confines of the Service. Some of this information should be shared with the bodies that are responsible for reviewing the activities of national security agencies.

> **Recommendation 24:** Amend section 11.01 and paragraph 11.07(1)(a) of the *CSIS Act such that* "publicly available dataset" is clearly and narrowly defined to cover statistics and data readily available from a source without payment, and explicitly exclude any data in which an individual may have a reasonable expectation of privacy.

[20] *In the matter of an application by [redacted] for warrants pursuant to sections 12 and 21 of the Canadian Security Intelligence Act, RSC 1985, c. C-23 and in the presence of the Attorney General and Amici and in the matter of [redacted] threat-related activities*, 2016 FC 1105.

Recommendation 25: Amend the *CSIS Act* such that the collection of publicly available datasets and foreign datasets can be authorized only where the Minister concludes that querying and exploiting any dataset in the class could lead to results that are relevant to the performance of the Service's intelligence, threat reduction or foreign intelligence roles.

Recommendation 26: Amend the *CSIS Act* such that where the Service to establish record-keeping requirements, those requirements should be shared with NSIRA and/or National Security and Intelligence Committee of Parliamentarians (NSICOP).

Recommendation 27: Amend the *CSIS Act* such that the rationale for collection/retention that must be recorded under the *CSIS Act* should be shared with NSIRA and/or NSICOP.

Threat Reduction Powers

CCLA remains concerned about the way in which CSIS's mandate has shifted in a manner that ignores the significant historical reasons for separating law enforcement and intelligence functions. We do not believe the case for granting threat reduction powers to CSIS has been made out by the government or that it has been demonstrated why better communication and cooperation between CSIS, the RCMP, and other law enforcement bodies is incapable of achieving the same goals.

The legal framework for the exercise of these powers established in Bill C-51 was deeply problematic and unconstitutional. The scheme as modified by Bill C-59 is an improvement: it establishes clearer contours around what actions are permitted and what is prohibited, and the warrant scheme appears to be *intended* to ensure that the *Charter* rights of individuals are respected. If CSIS is to continue to have these powers (a point we think has not been the subject of adequate debate), the scheme should certainly be improved further. In particular, changes should be made to clarify that threat reduction by CSIS is a last resort and to narrow the threat reduction measures available to the Service. In addition, amendments should ensure that questions of compliance with the law and the *Charter* are not left solely to CSIS.

Recommendation 28: Amend the requirement that CSIS consult with other federal departments or agencies to see if they can reduce the threat in subsection 12.1(3) of the *CSIS Act* to state that if a law enforcement agency is better placed to do so, CSIS should not pursue threat reduction.

Recommendation 29: The committee should carefully scrutinize the measures set out in subsection 21.1(1.1) of the *CSIS Act* to determine if any of them can be narrowed or refined.

For example, paragraph (g) allows CSIS to personate a person, other than a police officer, in order to take a measure referred to in any of paragraphs (a) to (f). At a minimum, CSIS should also be prohibited from personating a lawyer, a judge, a religious official, or a member of the press.

Recommendation 30: Amend the warrant scheme in the *CSIS Act* to require a warrant in *any* case where the measures set out in proposed s. 21.1(1.1) will be pursued by CSIS, regardless of CSIS's opinion on whether the measures would violate the law or *Charter.*

Security of Canada Information Disclosure Act Amendments

The *Security of Canada Information Sharing Act* ("SCISA") was one of the most profoundly flawed sections of Bill C-51. CCLA argued at that time, and continue to argue, that it is essential that the lessons of the Air India and Arar Inquiries are acknowledged, and that Canada's information sharing/disclosure practices are guided by principles of necessity, proportionality, and accountability. The amendments made in Bill C-59 fail to fully live up to these principles. The renamed *Security of Canada Information Disclosure Act* ("SCIDA") also, disappointingly, fails to completely incorporate many of the recommendations made by this Committee, and the Standing Committee on Access to Information, Privacy and Ethics (ETHI), after two extensive studies. CCLA's critique centres on four critical flaws, addressed below.

Definition of "activity that undermines the security of Canada"

The proposed changes to the definition of "activity that undermines the security of Canada" in section 2 of *SCIDA* leave concerns expressed regarding the breadth of that definition during every review of the *SCISA* largely unaddressed. As CCLA noted in our submissions on former Bill C-51, including "interference with intelligence activities" in the definition opens the possibility that encryption and other methods that individuals use to safeguard their personal information and protect their privacy may be inappropriately captured within a broad interpretation of such activities. We also remain concerned that constitutionally protected acts of advocacy, protest, dissent or artistic expression—particularly by environmental and Indigenous activists—will continue to be subject to information disclosures despite the addition of the qualifier "significant or widespread" to paragraph 2(f) which addresses interference with "critical infrastructure." For example, would a non-violent, long-term occupation of a resource extraction site be considered significant? Would a march scheduled for multiple Canadian cities be considered "widespread"? As the terms "significant" or "widespread" are vague and undefined, such questions make it difficult for the public to understand the scope of the law.

Further, the essential exception for acts of advocacy, protest, dissent or artistic expression is qualified in C-59 by the phrase "unless carried on in conjunction with an activity that

undermines the security of Canada."[21] This is incomprehensibly circular, and also entirely fails to capture the concerns expressed in previous studies of *SCISA*. While some commentators, including the influential Professors Roach and Forcese, expressed an opinion that violent forms of protest or dissent should be excluded from an exception for these activities, their explicit concern was with protest activities "intended to cause death or bodily harm, endanger life, or cause serious risk to health."[22] Any exception to the exemption from information sharing for protest and related activities should only be in cases where there is reason to suspect such serious harms are likely.

> **Recommendation 31:** Amend section 2(2) of *SCIDA* to read, "For the purposes of this Act, advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada unless carried on in conjunction with an activity intended to cause death or bodily harm, endanger life, or cause serious risk to health or public safety."

Thresholds for Disclosure and Retention

SCISA was soundly criticized for failing to set sufficiently high thresholds for information sharing; the standard in section 5(1) of *SCISA* required only that information be "relevant to the recipient institution's jurisdiction or responsibilities." Many witnesses noted this in submissions on former Bill C-51 and subsequently, this Committee, the Privacy Commissioner and the ETHI Committee have all made recommendations to raise this threshold.[23] The Privacy Commissioner has proposed, during this Committee's 2017 study and again during this current study of Bill C-59, a model of dual thresholds. In this model, disclosures may be made on a lower threshold, such as relevance to the exercise of a recipient institution's jurisdiction, but recipient institutions should be required to apply a necessity standard when evaluating whether or not they may use and/or retain information that is disclosed to them. CCLA believes the appropriate standard for disclosing and recipient institutions is one of proportionality and necessity but in the alternative, believes that the dual threshold model that this Committee endorsed in its May 17 report[24] is preferable to the provisions proposed in *SCIDA*.[25]

SCIDA largely leaves questions of retention of disclosed information to regulation,[26] which means that such rules will be subject to limited public scrutiny prior to approval. While regulation may be the appropriate way to set specific retention limits for different

---

[21] Proposed (Bill C-59) *Security of Canada information Disclosure Act*, s. 2(2).
[22] Craig Forcese and Kent Roach, Analysis and Proposals on the S*ecurity of Canada Information Sharing Act* (3 November 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2863364> at 4.
[23] Tanya Dupuis, Chloé Forget, Holly Porteous and Dominique Valiquet, Legislative Summary for Bill C-59: An Act respecting national security measures [Pre-Release], Library of Parliament (9 November 2017) Publication No. 42-1-C59-E at 29 [Tanya Dupuis et. al., "Legislative Summary for Bill C-59"].
[24] SECU, *Protecting Canadians and their Rights*, supra note 1 at Recommendation 26.
[25] Proposed (Bill C-59) *Security of Canada information Disclosure Act*, s. 5(1).
[26] Proposed (Bill C-59) *Security of Canada information Disclosure Act*, s. 10(1)(c).

institutions in differing circumstances, CCLA recommends that the legislation minimally contain a section prohibiting the retention of information by a recipient institution if analysis upon receipt determines it is not necessary for that institution to exercise its jurisdiction or carry out its responsibilities in respect of national security activities.

> **Recommendation 32:** Amend section 5(1) of *SCIDA* to require a threshold of necessity in subsection (a) for disclosures.
>
> **Recommendation 33:** Amend *SCIDA* to add a new section which specifies that receiving institutions may only use information disclosed to them that is necessary for the institution to exercise its jurisdiction or carry out its responsibilities in respect of national security activities.
>
> **Recommendation 34:** Amend *SCIDA* to prohibit the retention of information received under subsection 5(1) if it fails to meet a necessity threshold upon review by a recipient institution, when considered in relation to the recipient's jurisdiction and responsibilities in respect of national security.

Accountability Measures

Sections 9 and 10 of the *SCIDA* add record keeping requirements for disclosures to the legislation, and provide for NSIRA to receive copies of those records. This is a necessary addition to improve accountability and create at least the potential for appropriate review of decisions to disclose. While CCLA believes the mandate of the Privacy Commissioner of Canada does, and should, allow him to investigate disclosures under *SCIDA* (see below), and indeed, he has done so, we would like to see explicit provision for the Privacy Commissioner of Canada to also receive records created under section 9 of *SCIDA*.[27]

A critical gap in accountability remains in relation to the record keeping regime proposed under *SCIDA*. There are no record keeping requirements for recipient institutions: what information is disclosed, to whom, when, and how it is justified by the disclosing institution will be recorded, but whether the recipient institution deems it relevant for use in relation to its mandate, whether or how it is subsequently used, and whether it has been retained, will remain unrecorded, and unreported. To ensure full accountability for information disclosures under *SCIDA*, Bill C-59 should be amended to ensure that disclosures authorized by the Act may be reviewed throughout their life cycle, from disclosure, receipt, use, and retention.

> **Recommendation 35:** Amend subsection 9(1) of *SCIDA* to specify that every Government of Canada institution that

[27] Office of the Privacy Commissioner of Canada, 2015-2016 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*, September 2016, at 16-21, online: https://www.priv.gc.ca/media/4516/ar_201516_eng.pdf.

discloses and receives information under this Act must prepare and keep records.

Recommendation 36: As requested by the Privacy Commissioner in his December 7, 2017 submission to this Committee, add a new subsection to section 9 of *SCIDA*: "For greater certainty, the Government of Canada institution must also, on request by the Privacy Commissioner under s.34 of the Privacy Act, provide the Commissioner with a copy of any record requested that it prepared under subsection (1)."[28]

The *Privacy Act* and *SCIDA*

This Committee recommended in May 2017 that "the Government of Canada ensure that protections guaranteed under the *Privacy Act* are not abrogated by the *Security of Canada Information Sharing Act*, thus ensuring Canadians' privacy is protected."[29] *SCIDA* does not make the necessary clarification to provide this assurance. The seventh paragraph of the preamble to the Act specifically indicates that government institutions are accountable for disclosure that respects the *Privacy Act*, but it is not explicit in the operative text of the legislation. This is a concern, because under section 8(2)(b) of the *Privacy Act*, it specifies that personal information under the control of a government institution may be disclosed without consent "for any purpose in accordance with any Act of Parliament." Indeed, the background document produced prior to the national security consultation process preceding Bill C-59's introduction highlights this problem, as it specifically suggests that *SCISA* is a "lawful authority" for the purposes of that exemption.[30] To eliminate any ambiguity, it should be stated in the body of the *SCIDA* that the *Privacy Act* applies. Providing this clarity further provides the necessary assurance that the Privacy Commissioner of Canada may conduct investigations as per his or her mandate to ensure compliance with the *Privacy Act*.

Recommendation 37: Amend section 4 of *SCIDA*, "Guiding principles," to add a subsection (c) specifying that the protections of the *Privacy Act* are not abrogated by the *SCIDA* and that adherence to the *Privacy Act* is necessary for responsible disclosure of information.

---

[28] Office of the Privacy Commissioner of Canada, Appearance before the Standing Committee on Public Safety and National Security (SECU) on *Bill C-59, An Act respecting national security matters*, December 7, 2017, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_20171207/.
[29] SECU, *Protecting Canadians and their Rights,* supra note 1 at Recommendation 24.
[30] Public Safety Canada, *Our Security, Our Rights: National Security Background Document* ("Background Document"), at 27, online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf.

Secure Air Travel Act Amendments

General Comments

We share the view voiced by this committee in May of 2017 when it recommended "that the Government of Canada ensure effective safeguards in the Passenger Protect Program against any unfair infringements on individuals' legitimate right to liberty, freedom of movement, privacy and protections from discrimination on the basis of national or ethnic origin, religion, sexual orientation, or any other characteristic protected by law."[31] Unfortunately, this recommendation has not been meaningfully addressed in Bill C-59 and the *Secure Air Travel Act* continues to raise many concerns regarding civil liberties and equality rights.

While Bill C-59 makes a number of positive changes to the *Secure Air Travel Act* which may better protect children placed on the list, and which may help to reduce the number of "false positives," these fixes are ultimately minor in comparison to larger problems raised by the no-fly list. We support the bill's reversal of the rule for applications for administrative recourse, so that the Minister is no longer deemed to have decided against removal of a name from the list in situations where the Minister does not have sufficient information to make a decision, or simply fails to make a decision for other reasons.[32] However, the standard for adding an individual's name to the list—"reasonable grounds to suspect"—remains low given that listing may result in a severe restriction of the mobility rights guaranteed under section 6 of the *Charter of Rights and Freedoms*. Further, the Minister's ability to delegate her or his authority to limit these rights is far too broad.

> **Recommendation 38:** Amend the *Secure Air Travel Act* so that the Minister is only authorized to add an individual's name to the list on the basis of "reasonable grounds to believe" that the person will engage in the activities described in section 8.
>
> **Recommendation 39:** Amend section 7 of the *Secure Air Travel Act* to limit the scope of individuals to whom the Minister may delegate his or her powers, duties and functions under the Act.

Appeal Framework and Due Process

The *Secure Air Travel Act*'s remedial mechanisms remain similarly defective. Even if denied travel, individuals may never be explicitly informed that they are a listed person, which can frustrate their ability to seek recourse within the narrow window available to do so.[33] This is because the 60-day period begins on the day on which they were denied transportation, rather than the day on which they became aware of their status on the list.[34] There are also

---

[31] SECU, *Protecting Canadians and their Rights*, supra note 1 at Recommendation 38.
[32] Proposed (Bill C-59) *Secure Air Travel Act,* s. 15(6).
[33] The 60-day window is subject to the Minister's discretion to extend based on "exceptional circumstances that warrant it," see *Secure Air Travel Act,* s. 15(2).
[34] *Secure Air Travel Act,* s. 15(1).

more fundamental problems with the appeal mechanism, which replicates many of the same issues present in the security certificate context prior to 2008.[35] Proceedings may take place in secret,[36] appellants are only provided a discretionary summary of the intelligence and evidence used against them[37] (which may include hearsay[38]), and the judge is empowered to rely on evidence and information which has not been provided in that summary.[39] The appellant's right to be heard is not meaningful if she or he does not know the case to meet.[40] Moreover, the appellant is not afforded a special advocate with the ability to review and test the government's case. In addition to the clear issues with regard to due process and fundamental justice, these provisions also erode the separation of functions between judge and counsel in an adversarial system.

While being placed on the no-fly list undoubtedly comes with a different set of consequences than being named in a security certificate, both have the ability to substantially interfere with the constitutionally protected rights and liberties of an individual, including those protected under sections 6 and 7 of the *Charter of Rights and Freedoms* in a manner that cannot be saved by section 1. A no-fly list designation can also result in very serious practical costs to an individual's relationships and family life, compromise their employment, limit the professional opportunities available to them, and damage their reputation and community standing. This Committee recognized these profound issues in May when it recommended the use of special advocates in no-fly list proceedings, among other safeguards—and yet Bill C-59 does not address these concerns. It should do so by adopting this Committee's initial recommendation.

> **Recommendation 40:** Amend the *Secure Air Travel Act* to create a system for prompt and effective notice to individuals who have been denied air travel that they are, or are not, on the Canadian Specified Persons List, and that they do, or do not, share a name with an individual on the Canadian list. In the alternative, amend the *Secure Air Travel Act* to allow an individual who has been denied air travel to confirm the above with the Passenger Protect Inquiries Office, and amend subsection 15(1) such that the 60-day window only begins on the date the individual is made aware of their placement on the list.[41]
>
> **Recommendation 41:** Replace the appeals mechanism in section 16 of the *Secure Air Travel Act* with a system that:

---

[35] See *Charkaoui v Canada (Minister of Citizenship and Immigration)*, 2007 SCC 9 [*Charkaoui I*].
[36] *Secure Air Travel Act,* s. 16(6)(a).
[37] *Secure Air Travel Act,* s. 16(6)(c).
[38] *Secure Air Travel Act,* s. 16(6)(e).
[39] *Secure Air Travel Act,* s. 16(6)(f).
[40] See *Charkaoui I* supra note 35, e.g., at paras 29, 53; *Singh v. Minister of Employment and Immigration*, [1985] 1 S.C.R. 177 at p. 213; *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1 at para 123.
[41] SECU, *Protecting Canadians and their Rights,* supra note 1 at Recommendation 32.

a) ensures full disclosure of all information in the government's possession which is relevant to the listed individual's case; and
b) creates a mechanism for the appointment of a special advocate to protect the interests of the person who has appealed to have their name removed from the Specified Persons List, with the same powers and responsibilities to test and challenge that evidence as special advocates in the security certificate context.[42]

Finally, section 16(5) of the Act is drafted so that, after having found the decision to list an individual under section 15 unreasonable, the judge "may order that the appellant's name be removed from the list." This unusual discretionary power should be removed.

> **Recommendation 42:** Amend section 16(5) of the *Secure Air Travel Act* to read that "the judge shall order that the appellant's name be removed from the list."

Criminal Code Amendments

The proposed amendments to the *Criminal Code* in Bill C-59 give rise to a number of civil liberties concerns related to the terrorist entities list; the "terrorist speech" offence; the definition, seizure and deletion of "terrorist propaganda;" investigative hearings; warrantless arrest and recognizance with conditions; and terrorism peace bonds. In this section, we will address each of these issues in turn.

The Terrorist Entities List

The proposed amendments to section 83.05 of the *Criminal Code* appear to reduce the burden of proof for adding new entities to the terrorist entities list.[43] In order for the Minister to recommend an entity be added to the list, she or he must have reasonable grounds to believe that entity is one referred to in paragraph 83.05(1)(a) or (b)—in other words, that it has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity, or has knowingly acted on behalf of, at the direction of or in association with such an entity.[44] Proposed subsection 83.05(1.2) would allow the Minister, by regulation, to change the name of a listed entity, or add additional names by which it may also be or have been known, "if the Minister has reasonable grounds to believe that the listed entity is using a name that is not on the list." This change has the potential to increase the number of entities wrongfully placed on the list by virtue of the fact that a listed entity has simply *used* its name, even without knowledge, permission, or any substantial connection between the two groups.

[42] See also SECU, *Protecting Canadians and their Rights,* supra note 1 at Recommendation 37.
[43] Tanya Dupuis et. al., "Legislative Summary for Bill C-59," supra note 23 at 38.
[44] *Criminal Code,* s. 83.05(1) with proposed wording of paragraph 83.05(1)(b) (Bill C-59).

It is somewhat uncertain how the provisions related to mistaken identity[45] would protect innocent groups whose names have been appropriated by a terrorist entity.

It is not clear why it is necessary to extend the period for the Minister to issue a decision with regard to whether an entity should be removed from the list as proposed in subsection 83.05(3). Moreover, the ability of the Minister to extend this period indefinitely on the basis of a written agreement with the applicant is not likely to represent meaningful consent by the parties, given that if the applicant refuses to agree to an extension, the default outcome is simply to remain on the list. The Minister should be required to make an affirmative determination in order to maintain an entity's listed status following an application for removal.[46]

> **Recommendation 43:** Amend subsection 83.05(3) of the *Criminal Code* to read: "If the Minister does not make a decision on the application referred to in subsection (2) within 60 days after receipt of the application the Minister is deemed to have decided to recommend that the applicant be removed from the list.

The proposed amendment to paragraph 83.05(6)(a), which currently affords the judge the ability to examine "any security or criminal intelligence reports considered in listing the applicant," would be narrowed to any such reports "considered in the making of the decision on whether the applicant should remain a listed entity". This has the potential to dramatically reduce the scope of evidence and information available to the judge in a judicial review proceeding, thus hampering her or his ability to make an informed decision on judicial review.

> **Recommendation 44:** Amend paragraph 83.05(6)(a) of the *Criminal Code* to read "...any security or criminal intelligence reports considered in listing the applicant and in the making of the decision on whether the applicant should remain a listed entity."

As Professors Craig Forcese and Kent Roach have written, the fact that an entity's assets are frozen once listed poses a major practical barrier for those that seek to appeal their status on the list. They also point out the need for some guarantee that "those who work on the appeal as lawyers are not later accused of terrorism offences because of that work," noting that legislation in the United Kingdom provides such protection.[47] For example, it is possible that the broadly defined prohibition against participating or facilitating the activities of a

[45] *Criminal Code,* s. 83.07(1).
[46] This would also be consistent with the proposed framework for no-fly list appeals in Bill C-59 (in which the Minister is deemed to have decided to remove the applicant's name from the list after the delay to respond expires), see: Proposed subsection 15(6) of the *Secure Air Travel Act* (clause 134 of Bill C-59); see also SECU, *Protecting Canadians and their Rights*, supra note 1 at Recommendation 36.
[47] Craig Forcese and Kent Roach, "A report card on the national security bill," *Policy Options*, (22 June, 2017) <http://policyoptions.irpp.org/magazines/june-2017/a-report-card-on-the-national-security-bill/>.

terrorist group[48] could be construed in such a manner that it would expose the legal counsel of a listed entity to risk. The law should be clarified.

> **Recommendation 45:** Create a mechanism which allows a listed entity access to otherwise frozen funds for the purpose of paying for legal fees.

> **Recommendation 46:** Amend the *Criminal Code* to clarify that providing legal counsel to a "terrorist group" for the purpose of appealing that group's status as a listed entity does not constitute an offence under section 83.18 or otherwise.

Moreover, the procedure for judicial review in the context of listed entities replicates many of the due process and procedural fairness concerns associated with the no-fly list,[49] the pre-2008 security certificate process, and the security certificate process following the changes made in the *Anti-terrorism Act 2015*.[50] The wording of paragraph 83.05(6)(a) allows the Minister extraordinary discretion to withhold evidence and information that fails to support the Minister's conclusions—from the judge, the applicant, and the applicant's counsel alike. The applicant is then provided an incomplete and summary form statement of that already incomplete information,[51] and is not afforded a special advocate entitled to review or test that evidence. Wrongfully placing an entity on the list is likely to have very serious consequences for the individuals associated with that entity—including criminal law consequences with the potential to impact the liberty interests of an individual,[52] serious financial ramifications,[53] and the stigma of being identified with a terrorist group or cause.

> **Recommendation 47:** Amend the *Criminal Code* provisions related to the terrorist entities list to provide for the appointment of a special advocate with the ability to review and test all relevant evidence in proceedings related to the listing of terrorist entities.

The proposed amendments also dramatically diminish important accountability measures related to the terrorist entities list. These changes include:

---

[48] *Criminal Code,* s. 83.18.
[49] *Secure Air Travel Act*, ss. 15 et seq.
[50] See section entitled "Need to Amend the *Immigration and Refugee Protection Act*."
[51] *Criminal Code,* s. 83.05(6)(b).
[52] The definition of "terrorist group" in *Criminal Code,* s. 83.01(1) includes listed entities, and the term "terrorist group" is used to establish a number of offences in the *Criminal Code* such as s. 83.03 (providing, making available, etc., property or services for terrorist purposes), s. 83.08 (freezing of property provisions related to terrorist groups), s. 83.18 (participation in activity of terrorist group), s. 83.181 (leaving Canada to participate in activity of terrorist group), s. 83.2 (commission of offence for terrorist group), s. 83.201 (Leaving Canada to commit offence for terrorist group), and s. 83.21 (instructing to carry out activity for terrorist group).
[53] See *Criminal Code,* s. 83.08 (freezing of property) and 83.11 (obligations on third parties to audit control of property on behalf of listed entity).

1. Reducing the Minister's review obligations (by requiring reviews on a five-year basis[54] rather than a two-year basis as currently set out in subsection 83.05(9);
2. Removing the Minister's obligation to complete a review "as soon as possible and in any event, no later than 120 days after its commencement;"[55]
3. Modifying the Minister's obligation to publish notice of the completed review "without delay," and replacing that requirement with a five year period following completion of the review.[56]

> **Recommendation 48:** Do not replace the provisions set out in current sections 83.05(8) to (10) of the *Criminal Code* with proposed sections 83.05(8.1), 83.05(9) and 83.05(10).

The Terrorist Speech Offence

We are generally reassured by the government's attempted amendment of the terrorist speech offence,[57] though some outstanding issues remain. The offence, as adopted in the *Anti-terrorism Act*, *2015*, is a clear violation of the rights enshrined in sections 2 and 7 of the *Charter*. It criminalizes constitutionally protected expression, relies on a series of impermissibly low thresholds to establish the offence,[58] exposes individuals exercising constitutionally protected rights to a heightened risk of surveillance,[59] and has a chilling effect on freedom of expression and association, even in the absence of any enforcement. It captures statements made in private, and fails to include reasonable statutory defences for legitimate expression related to justice and education;[60] good faith opinion on a religious subject or an opinion based on a belief in a religious text;[61] religious, political, and ideological belief and opinion;[62] and the public interest.[63] Moreover, these provisions may ultimately undermine community-based deradicalization efforts, and thereby run at cross-purposes to the pressing objective of countering terrorism. Proposed subsection 83.221(1) rightly eliminates many of these issues by attempting to transform the provision into a "counselling" offence.

Unfortunately, the peculiar language of proposed paragraph 83.221(2)(b) directly undermines the government's proposed reform effort. It states that "an offence may be committed under subsection (1) <u>whether or not</u>…. the person counsels the commission of a <u>specific</u> terrorism offence." In other words, the provision replicates precisely the same constitutional issues as the phrase "terrorism offences in general" contained in the current wording of the *Act*—the provision is unconstitutionally vague and overbroad, in violation of

[54] Proposed (Bill C-59) *Criminal Code* s. 83.05(8.1).
[55] *Criminal Code,* s. 83.05(10).
[56] Compare proposed (Bill C-59) *Criminal Code* s. 83.05(10) with current s. 83.05(10).
[57] *Criminal Code,* s. 83.221(1).
[58] See "knowingly," "may," and "recklessness" in *Criminal Code,* s. 83.221(1).
[59] See *Criminal Code,* s. 185(1.1).
[60] See *Criminal Code,* s. 319(2).
[61] See *Criminal Code,* s. 163.1(6).
[62] See *Criminal Code,* s. 83.01(1.1).
[63] See *Criminal Code,* s. 319(3)(b).

section 7 of the *Charter*. While "terrorism offence" is defined, the scope of activity that would constitute a "non-specific" offence is unfixed and unknowable by both individuals and state agents charged with enforcing the provision, and appears to include counselling of conduct beyond the existing terrorism offences in the *Criminal Code*. The *actus reus* of counselling is "deliberate encouragement or active inducement of the commission of a criminal offence"[64]—it must go beyond mere advising or general encouragement.[65] In the absence of a specific offence to be induced, proposed section 83.221(1) is not only impermissibly vague, but continues to lie on the thin edge of criminalizing speech, rather than conduct.

Finally, we are of the opinion that even if this offence is amended it remains entirely unnecessary, given that counselling[66] (including counselling an offence which is not committed[67]) is already a criminal offence, as are as any number of other activities that would serve to support the operations of a terrorist group.[68]

> **Recommendation 49:** Repeal section 83.221 of the *Criminal Code*.
>
> **Recommendation 50:** If section 83.221 of the *Criminal Code* is not repealed, amend it to read "...to commit a <u>specific</u> <u>terrorism offence</u>," which would have the same meaning as in section 2.
>
> **Recommendation 51:** Remove proposed paragraph 83.221(2)(b) of the *Criminal Code*.

Seizure and Deletion of "Terrorist Propaganda"

While the definition of "terrorist propaganda" in subsection 83.222(8) has been amended to match the proposed changes to section 83.221, it is vulnerable to the same issues of vagueness and overbreadth, and should be amended accordingly.

> **Recommendation 52:** Amend the proposed definition of *terrorist propaganda* in subsection 83.222(8) of the *Criminal Code* to read "...that counsels the commission of a <u>specific</u> <u>terrorism offence</u>, other than an offence under section 83.221."

Section 83.223(5) and (6) allow the court to order a computer system's custodian to delete material determined to be "terrorist propaganda" and to order the destruction of the electronic copy in the court's possession. To the extent that "terrorist propaganda" constitutes evidence of an offence under 83.221(1) by definition (at least on a balance of probabilities), the court should not be allowed to destroy that evidence—which may be

[64] *R v Hamilton*, 2005 SCC 47 at para 29.
[65] *Ibid*; *R v Sharpe*, 2001 SCC 2.
[66] *Criminal Code,* s. 22.
[67] *Criminal Code,* s. 464.
[68] See e.g., *Criminal Code,* s. 83.18.

relevant to other related proceedings or exculpatory in nature.

Recommendation 53: Repeal subsection 83.223(6).

The provisions regarding the seizure and deletion of "terrorist propaganda" not only implicate the freedom to speak, but also the correlative right of individuals to hear, read, and generally receive information. Orders to provide information which would identify, locate, and de-anonymize an individual[69] will implicate that individual's right to be free of unreasonable search and seizure under section 8 of the *Charter.*[70] Extraordinary powers on the part of government to censor and de-anonymize speech should be accompanied by robust reporting and accountability requirements.

Recommendation 54: Introduce a requirement for the Attorney General of Canada to prepare a report to Parliament and to the public on the operations of sections 83.222 and 83.223 of the *Criminal Code,* on an annual basis, that includes:

a) The number of applications sought for the seizure of "terrorist propaganda," and the number obtained, by virtue of section 83.222;
b) The number of applications sought to order a custodian of a computer system, and the number obtained, by virtue of section 83.223. The report should be separated by type of order, whether production (s. 83.223(1)(a)), removal (s. 83.223(1)(b)) or identification (s. 83.223(1)(c)) respectively. It should also include the number of individuals implicated in identification orders and the number of instances of terrorist propaganda removed (assuming one order may comprise multiple instances of offending content).
c) The number of orders for deletion of "terrorist propaganda or computer data that makes terrorist propaganda available" made under subsection 83.223(5);
d) The number of orders to delete "terrorist propaganda or computer data that makes terrorist propaganda available" in the court's possession by virtue of subsection 83.223(6), if that subsection is not repealed;
e) A general description of each instance of "terrorist propaganda" subject to the aforementioned orders in the preceding year.

[69] As in *Criminal Code*, s. 83.223 (1)(c).
[70] See *Spencer* supra note 14.

Investigative Hearings

We support the proposed repeal of the investigative hearing provisions under section 83.28 and the related arrest provision under 83.29. The necessity of these provisions was never demonstrated, and they have never been used for their intended purpose.[71] The investigative hearing provisions undermine the legitimacy of the criminal justice system, distort the role of the judiciary, and are inconsistent with the rights and principles embodied in the *Charter of Rights and Freedoms.*

Warrantless Arrest and Recognizance with Conditions

Since their introduction in the *Anti-terrorism Act, 2001*, neither the warrantless arrest power nor the provisions to obtain a recognizance with conditions in section 83.3 have ever been used.[72] Along with the investigative hearing provisions, these were "exceptional" provisions subject to a sunset clause, and they should be allowed to expire in 2018 as anticipated, or be completely repealed.

If these extraordinary powers remain, the proposed amendment which raises the threshold in new paragraph 83.3(2)(b) and subsection 83.3(4) is a modest improvement. However, the low standard requiring only that the peace officer believes a terrorist activity "may" be carried out is inappropriately speculative and constitutionally insufficient: it should be raised. We support the clearer language with regard to subsequent extensions of section 83.3.[73]

> **Recommendation 55:** Repeal the *Criminal Code* provisions related to arrest without warrant for terrorist offences and the provisions to obtain a recognizance with conditions or allow them to expire subject to the sunset provision in subsection 83.32(1).
>
> **Recommendation 56:** If not repealed or expired, amend the low standard in paragraph 83.3(2)(a) of the *Criminal Code* ("...that a terrorist activity may be carried out") to a higher standard ("is likely to").

Terrorism Peace Bonds

In the *Anti-terrorism Act, 2015*, the previous government dramatically lowered the threshold to obtain a terrorism peace bond by changing the word "will" in subsection 810.011(1) such that it now requires only that a person "fears on reasonable grounds that another person

---

[71] Though used once in the Air India Inquiry.

[72] See Minister of Public Safety and Emergency Preparedness, *Annual Reports of the Minister of Public Safety Concerning Recognizance with Conditions: Arrests without Warrant*, Public Safety Canada (from 2013 to 2017) <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rrsts-wtht-wrrnt-2007-en.aspx>; Tanya Dupuis et. al., "Legislative Summary for Bill C-59," supra note 23 at 41.

[73] *Criminal Code*, s. 83.32(4).

may commit a terrorism offence." Given the significant impacts on the liberty interests of an individual subject to a terrorism peace bond—from onerous restrictions on travel, communication, and Internet use, to the use of curfews and forced counselling—this standard of proof is far too low.

While the constitutionality of peace bonds has been tested in other criminal law contexts, the potential scope of the conditions likely to arise in the terrorism context and the severe penalties for even minor breach, make terrorism peace bonds distinct.[74] As is the case for security certificates, these conditions may be so restrictive and wide-reaching in practice that imprisonment may be preferable to (and a lesser burden on the impacted person's family than) compliance with the peace bond.[75] Terrorism peace bonds are likely to be more all-encompassing, more prejudicial, and much less restricted than in other contexts, and this, coupled with the extraordinarily low standard of evidence, may call their constitutionality into question.

> **Recommendation 57:** Amend subsection 810.011(1) of the *Criminal Code* to read "fears on reasonable grounds that another person will commit a terrorism offence."
>
> **Recommendation 58:** Amend section 810.011 of the *Criminal Code* to limit the scope of conditions for terrorism peace bonds such that they are required to be narrowly tailored, reasonably necessary, and truly preventative in nature.

We support the new requirements for the Attorney General of Canada in proposed subsection 810.011(15) of the *Criminal Code* to report on the number of recognizances entered into under the sureties to keep the peace provision in section 810.011.

Need to Amend the *Immigration and Refugee Protection Act*

In the *Anti-terrorism Act, 2015*, the former government introduced a series of changes to the *Immigration and Refugee Protection Act* which removed important protections for named persons in security certificate proceedings. Those protections were adopted in 2008 following the Supreme Court's 2007 ruling in *Charkaoui v. Canada (Citizenship and Immigration)*, which found that the framework in place at the time—which allowed non-disclosure of evidence at certificate hearings—did not minimally impair the rights of persons named in certificates.[76] The Court affirmed that the individual named in a security certificate "must be given an opportunity to know the case to meet, and an opportunity to

[74] *R v Budreo* (2000), 46 OR (3d) 481 (CA); Kent Roach, "Be Careful What You Wish For? Terrorism Prosecutions in Post-9/11 Canada," (2014) 40:1 Queen's LJ at 114.
[75] Colin Freeze, "Under Constant Watch, Terror Suspect Seeks Return to Prison," *The Globe and Mail* (18 March 2009, updated 27 March 2017) <https://www.theglobeandmail.com/news/national/under-constant-watch-terror-suspect-seeks-return-to-prison/article20445712/>.
[76] *Charkaoui I* supra note 35, at 69 et seq.

meet the case," an impossible exercise in the absence of a coherent framework for the disclosure of relevant evidence.

Yet as of 2015, sections 83(1) and 85.4(1) of the *Immigration and Refugee Protection Act* have allowed the Minister to withhold information from a special advocate appointed to protect the interests of the person named in a security certificate, including information relevant to the government's case against the named person. These provisions are at odds with the Supreme Court of Canada's ruling in *Charkaoui I* and *Charkaoui II* regarding the scope of protection offered by section 7 of the *Charter* and the role of the special advocate in the security certificate system.[77] They are also at odds with the Supreme Court of Canada's ruling in *Canada (Citizenship and Immigration) v. Harkat* regarding section 7 protections and the judge's gatekeeper function.[78] The 2015 changes also gave rise to a number of other defects of due process and procedural fairness, affording the Minister virtually unfettered interim rights of appeal regarding orders made for disclosure of information. As the CCLA wrote to this committee in 2015, "while the protection of information touching on national security is certainly a pressing and substantial goal, the delays in judicial determinations that will be occasioned by broad appeal rights on behalf of the Minister may be highly prejudicial to named individuals. The appeal rights are also asymmetrical, putting the named person at a further disadvantage in cases where orders for disclosure have been refused."[79]

The preservation of Canada's national security interests is of critical importance. At the same time, the *Charter's* guarantee of a fair hearing and due process before an independent and impartial tribunal is a non-negotiable condition of a free and democratic society. The delicate balance struck by the courts to protect those rights prior to the *Anti-terrorism Act, 2015* should be restored. Security certificate proceedings must include safeguards commensurate to the potential severity of their impact on the lives of named persons—which can include deportation, detention, separation from family, and other forms of profound and irreparable harm. The provisions put in place by the *Anti-terrorism Act 2015* are unnecessary, and unreasonably threaten the constitutional guarantee that individuals not be deprived of life, liberty, or security of the person except in accordance with the principles of fundamental justice.

Bill C-59 does not address these problems at all. The government has stated that the purpose of referring Bill C-59 to committee prior to Second Reading was to allow for a greater scope of discussion, debate, and amendment. In our constitutional challenge and elsewhere, CCLA has argued that the *Anti-terrorism Act, 2015* amendments to the *IRPA* are an unconstitutional

---

[77] *Charkaoui I* supra note 35; *Charkaoui v. Canada (Citizenship and Immigration)* [*Charkaoui*, 2008 SCC 38; see also *Almrei (Re)*, 2009 FC 240 at para 43: "Such disclosure, it is to be remembered, consists of disclosure to the designated judge and the special advocate of all of the information in the possession of the Service concerning the named person."

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

[79] Canadian Civil Liberties Association, Submission to the Standing Committee on Public Safety and National Security regarding *Bill C-51, An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts (Anti-Terrorism Act, 2015),* March 2015 <https://ccla.org/cclanewsite/wp-content/uploads/2015/05/2015-03-17-C51-Submissions-Final-w-names.pdf>.

violation of the section 7 guarantee to a fair hearing before an independent and impartial tribunal. The security certificate regime has already been the subject of significant litigation, and this committee now has the opportunity to repeal those provisions as part of Bill C-59.

> **Recommendation 59:** Repeal all changes made to the *Immigration and Refugee Protection Act*, Division 9, by the *Anti-terrorism Act, 2015*.
>
> **Recommendation 60:** If the entirety of the 2015 amendments to the *IRPA* are not repealed, amend sections 83(1) and 85.4(1) of the *Immigration and Refugee Protection Act* in order to give special advocates full disclosure of all information in the government's possession relating to the individual's case.[80]

[80] See also SECU, *Protecting Canadians and their Rights,* supra note 1 at Recommendation 31.

Table of Recommendations

No.	Recommendation	Page
1	Amend subsection 4(7) of the *NSIRA Act* so that all members of the NSIRA hold office on a full-time basis in recognition of the significant volume of work they are expected to carry out. In the alternative, if part-time status is maintained, the number of NSIRA members should be increased to a minimum of six, plus a full-time Chair.	3
2	Amend the *NSIRA Act* to clarify that NSIRA is explicitly responsible for performing the same functions with respect to CSIS as is currently done by SIRC.	4
3	Amend the *NSIRA Act* to ensure that NSIRA is required to report publicly on the number of warrants issued under section 21.1 of the *CSIS Act* and the number of requests that were refused.	4
4	Amend sections 38-40 of the *NSIRA Act* to include language that clarifies that the reports that are made public should include *all* activities of NSIRA and unclassified versions of *all* findings and recommendations made by the Agency.	4
5	Amend the *NSIRA Act* so that NSIRA is responsible for reviewing, on a regular basis, the structure and information provided by the CSE in its annual report and is explicitly authorized to recommend the CSE include specific information in future reporting, including periodic inclusion of statistical information regarding the nature and scope of its activities.	4
6	Amend subsection 4(4) of the *Intelligence Commissioner Act* to set the remuneration of the Intelligence Commissioner in relation to the salary of a judge of the Federal Court, pro-rated to account for the fact that the position is part-time.	5
7	Remove subsection 4(2) of the *Intelligence Commissioner Act* so that the Intelligence Commissioner may only serve a single, non-renewable term. In this case, the term set out in subsection 4(1) should be made longer than five years.	5
8	Amend the *CSE Act* and the *Intelligence Commissioner Act* to require Intelligence Commissioner approval of active and defensive cyber operation authorizations granted by the Minister pursuant to sections 30 and 31 of the *CSE Act*.	6
9	Amend the *Intelligence Commissioner Act* to require the involvement of a special advocate, amicus, or similar entity to provide the Intelligence Commissioner with submissions in relation to the criteria for authorizations,	6

	amendments and determinations. This individual should be an independent, security-cleared lawyer with full access to all relevant information and evidence.	
10	Amend paragraph 21(1)(a) of the *Intelligence Commissioner Act* to require that the Intelligence Commissioner issue reasons even in circumstances where an approval is granted and allow for the reasons and order to be made public, to the fullest extent possible.	6
11	Amend the *Intelligence Commissioner Act*, the *CSIS Act*, and the *CSE Act* to create bilateral appeal rights to the Federal Court (applicable to the security service and the special advocate or similar entity) in respect of an approval or a refusal to approve an authorization by the Intelligence Commissioner.	6
12	Amend the *Intelligence Commissioner Act* to expand the range of options available to the Intelligence Commissioner by allowing him/her to attach conditions to authorizations in all cases.	6
13	Do not adopt the provisions in the *CSE Act* related to active cyber operations, and refer the issue for further study to evaluate the necessity and proportionality of these powers.	8
14	In the event that it is deemed to be necessary and proportionate based on a compelling and publicly defensible rationale, appropriate guidance should be included in the *CSE Act* to ensure that there are statutory safeguards in place to address situations when priorities within defensive and active cyber operation mandates conflict.	8
15	Amend section 25 of the *CSE Act* to include defensive and active cyber operations as activities also requiring measures to protect privacy.	8
16	Amend 61(b) of the *CSE Act* to require consultation with the Privacy Commissioner of Canada when making or revising regulations respecting the measures referred to in section 25 to protect privacy.	8
17	Amend the definition of "publicly available information" in section 2 of the *CSE Act* to: a) specify that it only includes information that has been published or broadcast for public consumption without restriction; b) remove the term "otherwise"; c) Limit the ability to purchase or subscribe to information from the definition, to specify that information for which remuneration is provided must be legally available to the general public, and that was legally obtained or created by the vendor (i.e. limit the purchase of information to "commercially available publications and broadcasts").	10

18	Amend section 24 of the *CSE Act* to add a limit to the activities listed in 24(1) namely: The measures shall be reasonable and proportional in the circumstances, having regard to the reasonably foreseeable effects on Canadians and people in Canada including on their right to privacy.	10
19	Amend the *CSE Act* to specify that publicly available information that identifies or is linked to an identifiable Canadian or person in Canada may only be disclosed if it is deemed essential to defence or security. Any such disclosures should be subject to independent review by NSIRA to ensure they meet that threshold.	10
20	Require Intelligence Commissioner approval in addition to current provisions for Ministerial authorization and the approval and/or informing of the Minister of Foreign Affairs for all active and defensive cyber operations.	11
21	Require Intelligence Commissioner approval of authorizations issued under sections 30 and 31 of the *CSE Act* in addition to the current reporting requirements to NSIRA mandated in s. 53.	11
22	Amend section 60 of the *CSE Act* to require CSE to include in its annual report how frequently active and defensive cyber operations are carried out.	11
23	Amend section 60 of the *CSE Act* to require CSE to include in its annual report the frequency at which it provides technical and operational assistance to other entities, and which agencies receive that assistance	11
24	Amend section 11.01 and paragraph 11.07(1)(a) of the *CSIS Act* such that "publicly available dataset" is clearly and narrowly defined to cover statistics and data readily available from a source without payment, and explicitly exclude any data in which an individual may have a reasonable expectation of privacy.	12
25	Amend the *CSIS Act* such that the collection of publicly available datasets and foreign datasets can be authorized only where the Minister concludes that querying and exploiting any dataset in the class could lead to results that are relevant to the performance of the Service's intelligence, threat reduction or foreign intelligence roles.	13
26	Amend the *CSIS Act* such that where the Service to establish record-keeping requirements, those requirements should be shared with NSIRA and/or NSICOP.	13
27	Amend the *CSIS Act* such that the rationale for collection/retention that must be recorded under the *CSIS Act* should be shared with NSIRA and/or NSICOP.	13
28	Amend the requirement that CSIS consult with other federal departments or agencies to see if they can reduce the threat in subsection 12.1(3) of the *CSIS*	13

	Act to state that if a law enforcement agency is better placed to do so, CSIS should not pursue threat reduction.	
29	The committee should carefully scrutinize the measures set out in subsection 21.1(1.1) of the *CSIS Act* to determine if any of them can be narrowed or refined. For example, paragraph (g) allows CSIS to personate a person, other than a police officer, in order to take a measure referred to in any of paragraphs (a) to (f). At a minimum, CSIS should also be prohibited from personating a lawyer, a judge, a religious official, or a member of the press.	13
30	Amend the warrant scheme in the *CSIS Act* to require a warrant in *any* case where the measures set out in proposed s. 21.1(1.1) will be pursued by CSIS, regardless of CSIS's opinion on whether the measures would violate the law or *Charter.*	14
31	Amend section 2(2) of *SCIDA* to read, "For the purposes of this Act, advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada unless carried on in conjunction with an activity <u>intended to cause death or bodily harm, endanger life, or cause serious risk to health or public safety</u>."	15
32	Amend section 5(1) of *SCIDA* to require a threshold of necessity in subsection (a) for disclosures.	16
33	Amend *SCIDA* to add a new section which specifies that receiving institutions may only use information disclosed to them that is necessary for the institution to exercise its jurisdiction or carry out its responsibilities in respect of national security activities.	16
34	Amend *SCIDA* to prohibit the retention of information received under subsection 5(1) if it fails to meet a necessity threshold upon review by a recipient institution, when considered in relation to the recipient's jurisdiction and responsibilities in respect of national security.	16
35	Amend subsection 9(1) of *SCIDA* to specify that every Government of Canada institution that discloses <u>and receives</u> information under this Act must prepare and keep records.	16
36	As requested by the Privacy Commissioner in his December 7, 2017 submission to this Committee, add a new subsection to section 9 of *SCIDA*: "For greater certainty, the Government of Canada institution must also, on request by the Privacy Commissioner under s.34 of the *Privacy Act*, provide the Commissioner with a copy of any record requested that it prepared under subsection (1)."	17
37	Amend section 4 of *SCIDA*, "Guiding principles," to add a subsection (c) specifying that the protections of the *Privacy Act* are not abrogated by the	17

	SCIDA and that adherence to the *Privacy Act* is necessary for responsible disclosure of information.	
38	Amend the *Secure Air Travel Act* so that the Minister is only authorized to add an individual's name to the list on the basis of "reasonable grounds to believe" that the person will engage in the activities described in section 8.	18
39	Amend section 7 of the *Secure Air Travel Act* to limit the scope of individuals to whom the Minister may delegate his or her powers, duties and functions under the Act.	18
40	Amend the *Secure Air Travel Act* to create a system for prompt and effective notice to individuals who have been denied air travel that they are, or are not, on the Canadian Specified Persons List, and that they do, or do not, share a name with an individual on the Canadian list. In the alternative, amend the *Secure Air Travel Act* to allow an individual who has been denied air travel to confirm the above with the Passenger Protect Inquiries Office, and amend subsection 15(1) such that the 60-day window only begins on the date the individual is made aware of their placement on the list.	19
41	Replace the appeals mechanism in section 16 of the *Secure Air Travel Act* with a system that: a) ensures full disclosure of all information in the government's possession which is relevant to the listed individual's case; and b) creates a mechanism for the appointment of a special advocate to protect the interests of the person who has appealed to have their name removed from the Specified Persons List, with the same powers and responsibilities to test and challenge that evidence as special advocates in the security certificate context.	19
42	Amend section 16(5) of the *Secure Air Travel Act* to read that "the judge <u>shall</u> order that the appellant's name be removed from the list."	20
43	Amend subsection 83.05(3) of the *Criminal Code* to read: "If the Minister does not make a decision on the application referred to in subsection (2) within 60 days after receipt of the application the Minister is deemed to have decided to recommend that the applicant <u>be removed from the list</u>.	21
44	Amend paragraph 83.05(6)(a) to read "...any security or criminal intelligence reports considered <u>in listing the applicant and in the making of the decision on whether the applicant should remain a listed entity."</u>	21
45	Create a mechanism which allows a listed entity access to otherwise frozen funds for the purpose of paying for legal fees.	22

46	Amend the *Criminal Code* to clarify that providing legal counsel to a "terrorist group" for the purpose of appealing that group's status as a listed entity does not constitute an offence under section 83.18 or otherwise.	22
47	Amend the *Criminal Code* provisions related to the terrorist entities list to provide for the appointment of a special advocate with the ability to review and test all relevant evidence in proceedings related to the listing of terrorist entities.	22
48	Do not replace the provisions set out in current 83.05(8) to (10) with proposed 83.05(8.1), 83.05(9) and 83.05(10).	23
49	Repeal section 83.221 of the *Criminal Code*	24
50	If section 83.221 of the *Criminal Code* is not repealed, amend it to read "...to commit a specific terrorism offence," which would have the same meaning as in section 2.	24
51	Remove proposed paragraph 83.221(2)(b) of the *Criminal Code*.	24
52	Amend the proposed definition of *terrorist propaganda* in subsection 83.222(8) of the *Criminal Code* to read "...that counsels the commission of a specific terrorism offence, other than an offence under section 83.221."	24
53	Repeal subsection 83.223(6).	25
54	Introduce a requirement for the Attorney General of Canada to prepare a report to Parliament and to the public on the operations of sections 83.222 and 83.223 on an annual basis that includes: a) The number of applications sought for the seizure of "terrorist propaganda," and the number obtained, by virtue of section 83.222; b) The number of applications sought to order a custodian of a computer system, and the number obtained, by virtue of section 83.223. The report should be separated by type of order, whether production (s. 83.223(1)(a)), removal (s. 83.223(1)(b)) or identification (s. 83.223(1)(c)) respectively. It should also include the number of individuals implicated in identification orders and the number of instances of terrorist propaganda removed (assuming one order may comprise multiple instances of offending content). c) The number of orders for deletion of "terrorist propaganda or computer data that makes terrorist propaganda available" made under subsection 83.223(5); d) The number of orders to delete "terrorist propaganda or computer data that makes terrorist propaganda available" in the court's possession by virtue of subsection 83.223(6), if that subsection is not repealed;	25

	e) A general description of each instance of "terrorist propaganda" subject to the aforementioned orders in the preceding year.	
55	Repeal the *Criminal Code* provisions related to arrest without warrant for terrorist offences and the provisions to obtain a recognizance with conditions or allow them to expire subject to the sunset provision in subsection 83.32(1).	26
56	If not repealed or expired, amend the low standard in paragraph 83.3(2)(a) of the *Criminal Code* ("...that a terrorist activity <u>may</u> be carried out") to a higher standard ("is likely to").	26
57	Amend subsection 810.011(1) of the *Criminal Code* to read "fears on reasonable grounds that another person <u>will</u> commit a terrorism offence."	27
58	Amend section 810.011 of the *Criminal Code* to limit the scope of conditions for terrorism peace bonds such that they are required to be narrowly tailored, reasonably necessary, and truly preventative in nature.	27
59	Repeal all changes made to the *Immigration and Refugee Protection Act*, Division 9, by the *Anti-terrorism Act, 2015*.	29
60	If the entirety of the 2015 amendments to the *IRPA* are not repealed, amend sections 83(1) and 85.4(1) of the *Immigration and Refugee Protection Act* in order to give special advocates full disclosure of all information in the government's possession relating to the individual's case.	29