Brief on Bill C-59, the *National Security Act, 2017*[1]

presented to
the Standing Senate Committee on National Security and Defence

by the
International Civil Liberties Monitoring Group

May 2019

[1] A longer version of this analysis of Bill C-59 can be found at https://iclmg.ca/documents/briefs/

Part 1: The *National Security and Intelligence Review Agency* (NSIRA) Act

The creation of a National Security and Intelligence Review Agency (NSIRA or Agency) with the ability to review all government activities related to national security is a very welcome development. The ICLMG has long supported the creation of such an overarching body, and believe it will have a significant, positive impact on transparency, accountability and effectiveness of Canada's national security activities. We also believe that this presents an important opportunity to learn from concerns that have been expressed regarding existing review agencies. By ensuring that these issues are not transferred to the new agency, the government can ensure that the NSIRA starts off on the right footing. We thus recommend:

1. a) That the minimum number of members of the NSIRA be set at 5 and the maximum number be increased to 8 (in addition to the Chair).
   b) That, in addition to nomination of NSIRA members being carried out in consultation with opposition parties, the final appointment be made by a 2/3 vote in the House of Commons to ensure the utmost independence from the government.
   c) That the membership will include people from diverse communities and multiple sectors – including those with an expertise in civil liberties and human rights.

2. That the NSIRA complaints mechanism be amended to apply to all national security activities, regardless of department. While the NSIRA will have the power to study all activities, individuals should also have the power to file complaints with an independent body regarding all national security activities. At a minimum, it should be modified to include both CBSA's and Global Affairs Canada's national security activities, as Canadian diplomatic and consular officers have played key roles in the mistreatment and torture of individuals such as Maher Arar, Abdullah Almalki, Ahmad El Maati and Muayyed Nureddin, all detained and tortured abroad.

3. That a more specific requirement be added under "Public Reports" to mandate a listing of each departmental study requested, and its result.

4. a) That the NSIRA be granted binding recommendation powers. This has been a particular issue regarding the Security and Intelligence Review Committee (SIRC), CSIS' current review body. A lack of clarity in public reports often make it difficult to ascertain what recommendations are being made, what aspects are or are not being implemented, and whether they have been effective in addressing the root of the complaint. It is understandable that some vagueness is necessary for operational reasons. By allowing SIRC to make binding recommendations, though, we could be more certain that the issues identified are being fully resolved. If we consider that the NSIRA plays — or, as we believe, should play — a similar role to a Commissioner of Inquiry, it is reasonable for it to have order-making powers.
   b) That the NSIRA's annual public reports include a mandatory follow-up and review of previous recommendations.

5. That the complaints investigation and reporting mechanisms be amended to ensure greater transparency and accountability; that complainants get access to all the

information necessary to their case; that all representations or recommendations made during the complaints investigation process are available to complainants; and that, to the greatest degree possible, complaint findings are released to the public.

6. Right now, neither current SIRC legislation nor proposed NSIRA rules provide for compensation or reimbursement of legal fees, even if abuse on the part of CSIS was found. In order for this review mechanism to be truly accessible and to repair the damage done by the national security agencies — and increase their accountability — the NSIRA should be able to rule on and offer redress to complainants.

Part 1.1: The *Avoiding Complicity in Mistreatment by Foreign Entities Act*

1. The current act should be replaced by legislation outlawing <u>any and all</u> use or sharing of information that would make Canada and its government agencies complicit in foreign mistreatment or torture and require mandatory yearly reporting by departments on how they fulfilled this obligation. This new Act does take the important step of mandating that all major departments and agencies involved in national security must have a ministerial direction regarding "avoiding complicity in mistreatment by foreign entities," but it does not establish what these guidelines must include.

   In Fall 2017, the Liberal government released revised ministerial directions regarding avoiding complicity is mistreatment by foreign entities. While an improvement on previous ministerial directions, these new regulations still allow, under certain circumstances, for Canadian agencies to use information obtained through mistreatment or torture; a completely unacceptable stance. There is also nothing in the Act that would prevent this or any future government from weakening ministerial directions, as we have seen in the past. The protection of rights must be enshrined, and not left to the whims of the government of the day or to be guarded by public pressure.

2. Annual reports on adherence to directions on avoiding complicity in mistreatment by foreign entities should not be subject to undue vetting. To that end, the provision allowing for their redaction based on injury to "international relations" should be removed.

Part 2: The *Intelligence Commissioner Act*

Much like the NSIRA, we welcome the proposal of a new Intelligence Commissioner (IC) and the important oversight role they will play before surveillance activities take place. However, much like the NSIRA, we believe there are ways the *Intelligence Commissioner Act* could be improved. Thus we recommend:

1. a) That the IC be nominated by the Governor in Council, but approved by a 2/3 vote in the House of Commons. to ensure independence from the government.
   b) That the IC be appointed on a full-time, rather than a part-time basis.
   c) That the pool for selection should also include active superior court judges to offer more choices.

2. That the NSIRA be mandated to include a section regarding the work of the Intelligence Commissioner, including an external review of their work.

3. That (a) the IC be able to impose conditions on approved authorizations, and (b) that IC approval be necessary in addition to the consent of the Minister of Foreign Affairs for all defensive cyber authorizations. If there are to be any active cyber authorizations, more rigorous oversight is required. This is discussed further in the section on the *CSE Act*.

Part 3: The *Communications Security Establishment* Act

The ICLMG would like to highlight the importance of finally legislating the Communications Security Establishment (CSE), considering it has been active, in one form or another, since World War II. However, we would also note that legislating the CSE's powers should not just be accepted based on the fact the agency has been carrying out this work for more than 70 years. The federal government must demonstrate to the public that these existing powers — in addition to the new powers introduced by Bill C-59 — are necessary to keep Canadians safe and that they respect the *Charter of Rights and Freedoms*. Furthermore, these new and old powers should not have been in the same 150-page omnibus bill with improvements such as new oversight and review mechanisms, as well as changes to the No-Fly List. The adoption of these changes should not be conditional on approving legislation such as the *CSE Act*.

General recommendations:

A. That the Intelligence Commissioner be empowered to review all of CSE activities.
B. That the government take steps to further narrow the scope of the CSE's surveillance and cyber activities overall.
C. That, to ensure accountability of the CSE, the independence and transparency of the work of the Intelligence Commissioner be strengthened and, to the greatest amount possible, the CSE's powers and authorizations be narrowly defined.

Specific recommendations:

1. That the CSE's mandate continue to be limited to defence and national security, and thus active cyber operations should not be added. In any case, "international affairs" should be removed from the CSE's mandate. "Active" cyber operations cannot be justified for defence or security reasons – especially when the potential retaliation for such cyber attacks could endanger our security. We also strongly disagree that "international affairs" is a sufficient reason to launch any kind of cyber operations.

2. That more must be done to ensure that the CSE's activities <u>actually</u> do not target or implicate Canadians or people in Canada. But if they do, a warrant should be required for any activities that could implicate Canadians or people in Canada, even if the activities are not directed at them, including activities related to the CSE's technical and operational assistance to other law enforcement and intelligence agencies such as the RCMP and CSIS.

3. Metadata is often dismissed as not being private information under the incorrect pretense that it does not reveal personal details. The *CSE Act* should define metadata; strongly

limit its collection, use and retention; and require a warrant for metadata collection.

4. While Ministerial authorizations will need to be approved by the Intelligence Commissioner, it is insufficient. Approvals such as this, conducted in secret, can and have resulted in secret legal analysis, untested outside of the national security sphere. We need only look to the United States for a cautionary tale: similar mechanisms there — such as the FISA court — have a track record of rubber-stamping warrants, becoming more and more permissive over time, and allowing for surveillance to be deployed on massive scales, violating the rights of millions of Americans. The only reason we know this is because of Edward Snowden. A similar system in Canada could very well have similar results. We therefore recommend:

   a) That Ministerial Authorizations of surveillance operations be restricted to a precise and narrow target
   b) That the targeting of unselected information be removed from the *CSE Act,* or, at a minimum, that the Intelligence Commissioner be granted the powers to rule that such actions are disproportionate, and/or impose binding limits.
   c) That information collected should not be retained longer than *necessary* to fulfill the intended objective.
   d) That Ministerial Authorizations be reduced to the amount of time *necessary* to fulfill the intended objective, and any extension and changes should only be done with the examination and approval of the Intelligence Commissioner.
   e) That the Canadian government not engage in mass surveillance. Barring this, that it at a minimum questions the existence of mass surveillance, and provides evidence to the public as to the effectiveness and necessity of surveillance – especially if it is approved in secret.

5. The *CSE Act* stipulates that the CSE "can acquire, use, analyse, retain or disclose publicly available information." This is too vague and broad, and will allow the unnecessary collection of troves of information that could lead to the creation of profiles on thousands of Canadians, as the Privacy Commissioner of Canada has already warned. The wording would also allow the CSE to acquire this publicly available information via problematic means, such as leaked information from a hack. Buying information from data brokers — with our tax dollars — thus encouraging an industry based on syphoning up private information, should be excluded under the Act. The CSE has argued that this provision would simply allow the collection of public reports and information that is necessary to their work, but unrelated to their mandate. If that is true, it should be specified as such. We therefore recommend:

   a) That the definition of “publicly available information” be limited in application to commercially available publications and broadcast, that further restrictions be placed on any collection of such data.
   b) That the CSE may only acquire, use, analyze and retain publicly available information if such information falls within a dataset approved by the Intelligence Commissioner.

6. That greater restrictions be imposed on the CSE's carrying out of work in support of the *Investment Canada Act,* including limits on how information is collected, retained, analyzed and disposed of.

7. That incidentally acquired information can only be retained so long as it is necessary for protecting the security of people in Canada.

8. The *CSE Act* stipulates that the CSE must ensure that measures are in place to protect Canadians' privacy when information about them is incidentally collected and the information is publicly available, but it fails to mention what those privacy protections are and how they will be determined. Moreover, privacy protections in place before Bill C-59 was introduced did not stop the agency from carrying out activities, revealed by Edward Snowden and the media, that clearly disregarded the privacy rights of Canadians, as well as non-Canadians, in Canada and abroad. To name a few problematic actions, the CSE:
    - Allowed the NSA to create a "backdoor" in an encryption key used worldwide;
    - Spied on Canadians using public WiFi networks, including in airports;
    - Captured millions of downloads daily;
    - Engaged in mass surveillance of file-sharing sites;
    - Developed cyber-warfare tools to hack into computers and phones all over the world;
    - Shared information on Canadians with its foreign partners without proper measures to protect privacy (and the data was later erased from the agency's system making it difficult to find out the number of people impacted by the privacy breach).

    Therefore we recommend that:
    a) The *CSE Act* enshrines strong privacy protections around CSE's activities into law.
    b) The problematic actions of the CSE, including those mentioned above, be outlawed.

9. That information gathered in order to protect information infrastructure from mischief, unauthorized use or disruption not be disclosed for any other purpose.

10. That, regarding designating persons for the purpose of disclosure of Canadian identifying information, the Minister of Public Safety should report such a designation and the reasons for the disclosure to either the Intelligence Commissioner or Privacy Commissioner, who may then rule on it. These reports should also be provided to the NSIRA.

11. a) That all arrangements with foreign countries be strongly regulated, limited and approved by the Intelligence Commissioner.
    b) That when sharing information with a foreign country, it is necessary for the Intelligence Commissioner to explicitly determine the likelihood that bodily harm – including mistreatment or torture – could be at play in any arrangement.
    c) That the Intelligence Commissioner include an analysis of what impact an

authorization may have on mistreatment or torture in their written decisions.

12. That judges be prevented from ordering that confidentiality of information or of any person or entity that has assisted or is assisting the CSE be respected if it hinders due process.

13. That the practice of the Five Eyes spying on each other, and the use of such information to skirt rules prohibiting the surveillance of Canadians or people in Canada, be outlawed.

14. a) That the definition of possible cyber operations be narrowed to only allowing activities that are strictly necessary to protect the safety of people in Canada.
    b) That cyber operation powers be considered akin to military actions and should be discussed publicly, and that further restrictions should be placed on them, including oversight and reporting from the Intelligence Commissioner.
    c) That cyber threats not be used to expand domestic surveillance powers.
    d) That the creation and use of any cyberweapons be strongly limited, as they can and have been leaked, making us the targets of criminals.
    e) That cyber security initiatives have genuine oversight and be more transparent.
    f) That cyber operations only allow defensive purposes, not offensive cyberattacks.
    g) If active cyber operations are still allowed, that they require the approval of the Intelligence Commissioner or of Parliament.

Part 4: Amendments to the *CSIS Act*

Bill C-59 would bring changes in an attempt to limit threat reduction powers, to make them *Charter* compliant, and to increase after the fact review of CSIS' threat reduction activities. Despite these proposed changes, we continue to firmly oppose CSIS being granted these extraordinary powers similar to those of a law enforcement agency but without the transparency, accountability or adversarial nature of our criminal justice system. It is imperative that we remember the lessons of the McDonald Commission, which concluded that security intelligence must be separated from law enforcement activities in order to protect our civil liberties. More precisely, the changes in C-59 are concerning because:

- CSIS should not determine whether a particular action meets the standard of limiting a *Charter* right and thus requires a warrant;
- requiring seeking judicial authorizations on a case-by-case basis to limit a *Charter* right is a significant departure in Canadian law, not comparable to search or surveillance warrants. And even if it was seen as a judicially acceptable practice, the results would still be kept secret, creating what Professors Forcese and Roach have described as a "secret jurisprudence." This result would continue to pose an important threat to Canadians' fundamental rights and freedoms.
- The proposed solution to this secrecy, in part, are rules requiring CSIS to report on its threat reduction activities to the NSIRA. While on paper the new NSIRA would have broad powers of review, much of what they would investigate and eventually report back to government and to CSIS would remain secret. It means that the public, civil liberties advocates, and the people targeted by threat reduction activities, or even most

parliamentarians, still do not have the power to examine, challenge or discuss these invasive powers.

- Further, SIRC, in its 2016-17 report, reported that it believes CSIS up to this point has been following proper procedure in engaging in threat reduction activities. CSIS also reported to SIRC that it has not yet sought judicial authorization for any threat reduction activity. While on the surface this seems positive, the public is still unaware of the nature of CSIS threat reduction activities, which could still be very invasive even if CSIS has deemed them to not require a warrant. We have seen that not only do review agencies not necessarily have access to all the information they need, but that CSIS has also deliberately misled or withheld crucial information from them and the courts. If we look to the past, there is a clear list of incidents and reports that raise questions about whether review will be effective in reigning in these new, invasive powers. For example, in 2016, a Federal Court judge found that CSIS had illegally retained and analyzed data on people who posed no threat to national security, for ten years. The judge found that not only CSIS failed to inform the court of this activity, but that while SIRC was informed of the activity, no flags were raised; leading to serious concerns about CSIS' transparency and SIRC's efficiency.

We therefore recommend that:

1. C-59 be amended to repeal CSIS' current threat reduction powers.

As mentioned above, in 2016 the Federal Court found that CSIS had been illegally retaining and analyzing data related to non-target individuals. At the time, the decision was not challenged, but it was noted that the government left the door open for an eventual legal solution that would allow for CSIS to continue this kind of collection, retention and analysis. The provisions in Bill C-59 to create new classes of datasets that CSIS can collect, retain and query appear to be such a proposed solution. Although safeguards are included in the bill, they are insufficient and we hold serious reservations about the very existence of these new powers.

We strongly oppose the government's decision to allow CSIS to broaden the scope of its surveillance activities, from targeting specific people under investigation to targeting entire classes of datasets. This is a clear change in the operations of CSIS to one of potential mass surveillance, collecting vast amounts of information about Canadians and non-Canadians. CSIS and the government have not demonstrated the necessity of these dangerous powers. For all these reasons, we recommend the following:

2. That collecting entire datasets be removed from the bill and CSIS' surveillance activities be only targeted to specific people and threats.
3. If the collection of datasets is kept in the bill, that authorizations for Canadian datasets should be reduced from two to one year, with the possibility of requesting an extension in writing.
4. That documentation of all queries of Canadian and foreign datasets (including reasons for and results) be shared with the NSIRA for review within 30 days.
5. That the Federal Court have the power not only to examine the relevance of a query but also any eventual use of that query in order to ensure that ramifications of an illegal query are addressed.

6. That authorizations for foreign datasets be reduced from five to one year with the possibility of extension for one more year granted only by the Intelligence Commissioner.
7. That querying datasets for foreign intelligence purposes be only allowed if strictly necessary.
8. That "publicly available information" be limited to commercially available publications and broadcasts, and its collection only be approved by the Intelligence Commissioner if strictly necessary for CSIS to carry out its mandate.

Bill C-59 will be granting CSIS agents or individuals at their direction, immunity for "acts or omissions that would otherwise constitute offences." Essentially, this will grant them the permission to break Canadian law in the pursuit of their activities. Firstly, we have seen no public justification from the government about the need for such new powers to be granted. Secondly, when law enforcement officials were granted these powers in 2001 (in Bill C-24), the proposal was already controversial. At the time, the Canadian Bar Association raised serious concerns, calling it "antithetical to the rule of law." These concerns are even more serious when such powers are given to intelligence agents operating in secret. As with CSIS' threat disruption powers, the issues with granting these powers to CSIS officers are compounded by the fact that, even after the fact, CSIS' actions are unlikely to be revealed or challenged in open court.

Therefore, we recommend:

9. That CSIS agents, and individuals at their direction, not be granted immunity for "acts or omissions that would otherwise constitute offences".

Part 5: *Security of Canada Information Disclosure Act*

Bill C-59 states that "disclosure will not affect any person's privacy interest more than reasonably necessary." This is overly broad and subjective.

Bill C-59 also clarifies the definition of activities that undermine the security of Canada, which triggers a department being allowed to disclose our private information to another department. It says that to qualify as "undermining the sovereignty, security or territorial integrity of Canada", an activity should constitute "significant and widespread interference with critical infrastructure." This may appear to be an improvement, but in reality, the bill could still cover environmental and Indigenous acts of dissent, which often entails blocking bridges and roads to protect water and land from dangerous energy projects that communities have not consented to. It could also potentially encompass activities related to Indigenous land claims if they are defined as "undermining the sovereignty and territorial integrity of Canada."

Furthermore, SCIDA would apply to "conduct that takes place in Canada and that undermines the security of another state." We are concerned that this could allow the sharing of information on individuals involved in international solidarity campaigns such as the Boycott, Divestment and Sanction (BDS) movement against products coming from illegal Israeli settlements.

Moreover, the addition of "except if done in conjunction with activity that undermines the security of Canada" to the "exception for art, protest, advocacy or dissent" is a step backward from Bill C-51. As we have shown above, various forms of protest and dissent could be

considered as an activity that undermines the security of Canada, therefore triggering SCIDA's powers. Therefore we recommend:

1. SCISA should be rescinded and be replaced by strong privacy protections regulating the sharing of information for national security purposes.
2. Barring this, we recommend that the definition activity that undermines the security of Canada in section 2 be replaced with the following:
   activity that undermines the security of Canada means any activity that threatens the lives or the security of people in Canada or of any individual who has a connection to Canada and who is outside Canada. For greater certainty, it includes
   (a) interference with the capability of the Government of Canada in relation to defense or public safety;
   (b) changing or unduly influencing a government in Canada by force or criminal means;
   (c) espionage, sabotage or covert foreign-influenced activities;
   (d) terrorism;
   (e) proliferation of nuclear, chemical, radiological or biological weapons;
   (f) significant or widespread interference with the global information infrastructure;
   (g) conduct that takes place in Canada and that threatens the lives or security of people in another state.
3. That section 2(1) be replaced with, "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." (This is a recommendation but forward by the CCLA which we support)
4. That an exception also be included to cover actions relating to Indigenous sovereignty, land claims, or title rights.

Part 6: Amendments to the *Secure Air Travel Act*

The changes to the SATA may lead to an eventual improvement in handling false positives and ensuring privacy of travelers' information. However, these amendments do not take the full steps needed to bring about redress for "false positives". Instead, Bill C-59 simply lays the groundwork for possible future regulations. The government should include clear guidelines for the creation of a redress system for false positives. One possibility would be granting the Passenger Protect Inquiries Office (PPIO) the mandate to take immediate steps to establish and manage a redress system. However, as we outline further below, this redress system – already described as complicated and costly – would not be needed if it were not for a flawed and unnecessary no-fly list program. There are several major problems with the No Fly List:

- It undermines the right to due process for individuals on the list through a lack of transparency and access to information;
- It lacks a fair appeal process;
- It allows unregulated information-sharing with foreign entities which can lead to human rights abuses;
- Its efficiency and necessity have never been demonstrated.

The serious questions of lack of due process, infringement on Charter-protected mobility rights, racial profiling and undue hardships, combined with the complete lack of data from the government regarding the effectiveness of the No Fly List program leaves us no other choice but to conclude that the system should be completely repealed. If a person is a threat to the safety of others, the government should act using existing criminal code procedures that follow due process. Thus we recommend:

1. That the Safe Air Travel Act should be repealed and the Passenger Protect Program be ended.
2. That, barring this:
   a) The government include clear guidelines for the creation of a redress system for false positives.
   b) Decisions to add an individual to the list should be reviewed and approved by a court.
   c) Individuals should be given written notice that they have been listed.
   d) That in defending their listing, an individual and their counsel, have full access to the information and evidence being presented in support of the listing.

Part 7: Amendments to the *Criminal Code*

We recommend:
1. That, because "counselling" is already an offense in the criminal code, the repetitive offense of "counselling terrorism offenses" be removed.
2. That, similar to the changes to preventative detention, the threshold for peace bonds should be increased to "necessary" to prevent a crime.
3. That Bill C-59 should repeal the "Terrorist Entities Listing" in favour of simply using laws that already prohibit organizations from taking part in criminal activities.

Part 9: Review of the *National Security Act*

C-59 plans a review of Bill C-59 in six years. This is an important safeguard, and we would suggest reducing it to five years for the new oversight and review mechanisms — since it will take time to establish the new offices, etc. — and to three years for the new CSIS and CSE powers. It will be important to ensure that this review happens in an open, public manner, with clear timelines for gathering input from all stakeholders. Recommendations of the review should be binding and fully implemented.

What is missing from Bill C-59

1. A strong review mechanism should look at the CBSA and its activities outside of national security.
2. Provisions that put an end to the security certificate regime should be added.
3. The Tipoff US/Canada (or TUSCAN) database is another even more secretive watch list that extends to every air, land and sea entry in Canada and has no clear redress process. C-59 should include a provision outlawing its use by Canadian border guards.
4. C-59 should include a provision outlawing the use of the US No-Fly List by airlines for flights that are not going to the US and/or are not passing through its airspace.