Feb. 9, 2024

Public Safety Canada
269 Laurier Avenue West
Ottawa, ON K1A 0P8
Sent by email to: ps.publicsafetyconsultations-consultationssecuritepublique.sp@ps-sp.gc.ca

Re: Submission regarding the consultation on "Enhancing measures to counter foreign interference: Whether to amend the *Canadian Security Intelligence Service Act*"

To whom it may concern,

I am pleased to submit the following submission regarding the consultation on whether to amend the *Canadian Security Intelligence Service Act* in the context of addressing foreign interference on behalf of the International Civil Liberties Monitoring Group coalition (ICLMG).

The International Civil Liberties Monitoring Group (ICLMG) is a Canadian coalition of 45 organizations founded in 2002, following the adoption of Canada's first *Anti-terrorism Act*. Over the ensuing two decades we have worked with our members, partner organizations, impacted communities and law makers to defend civil liberties in Canada against national security over-reach and abuses in the name of countering terrorism.

While issues of counter-terrorism and countering foreign interference are distinct, there are also many similarities, particularly in the kinds of legislative changes being considered and the national security-related tools being proposed. Moreover, as we highlight in our submission, many of the proposals being brought forward would not be limited in their impact to countering foreign interference but have wide-ranging impacts on CSIS' capabilities across its mandate.

We thank you for taking the time to consider our recommendations and feedback and look forward to discussing them more with you in the coming weeks and months.

Sincerely,

Tim McSorley
National Coordinator
International Civil Liberties Monitoring Group

Issue #1: Whether to enable CSIS to disclose information to those outside the Government of Canada for the purpose of increasing awareness and resiliency against foreign interference

What Do You Think?

1. Should CSIS be authorized to disclose information to those outside of the Government of Canada to build resiliency against threats, such as foreign interference?
2. In your view, what considerations should apply to the sharing of information with those outside of the Government of Canada about the threats they face? What type of limits should there be on when and with whom CSIS can share information?

Events over the past two years have demonstrated that the federal government's approach to addressing concerns around foreign interference are inadequate, including how, why and with whom to share information. A key issue is the framing of "foreign interference" itself: while there are documented examples of foreign governments taking an interest and attempting to influence democratic processes in Canada, questions remain regarding the breadth and impact of such activities, and what responses are merited. This is at the heart of the current Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, led by Justice Marie-Josée Hogue. Other key aspects of "foreign interference" include threats and harassment of diaspora communities by foreign states in order to limit their activities, corporate espionage and theft, and academic interference, among others.

These are clearly serious issues that must be addressed, particularly concerning threats to individuals and interference with essential services that put at risk the health and safety of people across Canada. However, we are concerned that the overall approach to this issue to date has focused on greater securitization, greater police and intelligence agency powers, and has raised concerns around the targeting and marginalization of specific communities and worries of a new

"McCarthyism" focusing on individuals with ties to particular countries based on political divisions and not actual threat.

It is important not to minimize the threat that foreign governments that do not respect human rights can pose to individuals in Canada, as well as their families and close ones abroad.

We remain concerned, though, around the politicization and vagueness of terms like "foreign interference" and how they can be usurped to achieve and support goals unrelated to ensuring security of individuals in Canada. Nor can we ignore, like the documented discrimination and profiling we see in Canada's efforts to address terrorism threats, that attempts to counter foreign interference – as demonstrated in recent public discourse – can lead to racial, religious and political profiling.

It is important that there is clarity around the issue meant to be addressed to ensure an appropriate approach. This includes being able to determine what role security agencies should play, and what role other government departments should take.

Specifically around CSIS being granted new powers to share information in order to build resiliency and protect against threats of foreign interference, we would raise some key concerns:

Firstly, we believe more evidence is required overall in order to justify granting CSIS greater information sharing powers with other organizations and entities to address foreign interference.

In its 2019 Annual Report, the National Security and Intelligence Committee of Parliamentarians (NSICOP) reported that they found overall government efforts to share information on foreign interference with outside partners were "ad hoc" as well as "inconsistent and uninformative."[1] While NSICOP did recommend that legislative changes and expansion of security clearances be considered, the report also suggested non-legislative approaches, including a more strategic, whole-of-government approach to reaching out to the public, to institutions and to other levels of government.

NSICOP rang the alarm again in its 2022 annual report (released in Spring 2023), raising concerns that the government has yet to respond to their recommendations.[2] The government responded with an action plan that included proposals for a more whole-of-government approach and new initiatives to engage the public.[3] However, the report lacked specifics on CSIS and CSE efforts to engage the public and civil society between 2019 and 2023, and the focus seemed to remain on security service activities, rather than engaging other branches of government. Given

[1] National Security and Intelligence Committee of Parliamentarians, *Annual Report 2019*. Online: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf
[2] National Security and Intelligence Committee of Parliamentarians, *Annual Report 2022*. Online: https://www.nsicop-cpsnr.ca/reports/rp-2023-07-19-ar-2022/NSICOP-2023-Annual-Report-English.pdf
[3] Government of Canada, *Countering an evolving threat: Update on recommendations to counter foreign interference in Canada's democratic institutions*. 6 April 2023. Online: https://www.canada.ca/en/democratic-institutions/services/reports/countering-evolving-threat.html

that this action plan was released less than a year ago, no update has yet been shared about the impact or implementation of the proposals. That said, it remains clear that there are other options open to the government beyond classified briefings from CSIS that should be explored.

This is further complicated by the fact that CSIS does in fact share threat assessment related information with the private sector. While stakeholders in the private sector have argued that existing restrictions remain too tight, outlets such as the *National Observer* have reported on regular classified briefings between national security agencies, including CSIS, and national resource companies.[4] During these meetings, national security officials provided "intelligence briefings to select energy representatives so they are able to implement the required security precautions to protect their assets. The briefings also provide a forum for the private sector to brief the Canadian intelligence and law enforcement community on issues we would not normally be privy to." Attendees at these briefings apparently had "Level II (Secret) Security Clearance." The ability for CSIS and the RCMP to share this kind of information appears to contradict the need for expanded information sharing power; alternatively, this raises questions of whether such briefings should have been possible in the first place.

Second, there are ongoing concerns regarding systemic bias and racism in Canada's approach to national security and counter-terrorism. This includes, for example, the undue targeting and profiling of the Muslim and Arab community in Canada as national security threats. Our work has documented how a sole focus on "national security" based solutions can often cause more divisions in society rather than address root causes of division or violence. While recognizing that the issues involved in addressing foreign interference are not exactly the same as those addressing terrorism threats, we have already seen similarities in, for example, anonymous leaks of unsubstantiated information alleging foreign interference by specific individuals or entire communities, some of which have been disproven or continue to remain unsupported by public evidence.

We can also see examples in the apparent format and content of the security briefings already being provided to natural resource companies. In general, the existence of these meetings has been kept secret, and the nature of what is shared is kept confidential. While it is understandable that aspects of these meetings take place behind closed doors, the complete lack of disclosure raises concerns around transparency and accountability around how these meetings are conducted, what information is shared and how threats are framed. For example, the National Observer reported in 2017 that "items of discussion include issues such as "security challenges presented by Radicalized Individual Groups to Canada's Energy Sector" and "Extremist Activities within Aboriginal Communities", and topics such as "Improvised Explosive Devices", or on specific projects, such as the oilsands and Northern Gateway pipeline." This one-sided approach to an important issue is clearly unacceptable. We would be equally concerned that

[4] Livesey, B. "Canada's spies collude with the energy sector," 18 May 2017. *National Observer.* Online: https://www.nationalobserver.com/2017/05/18/news/canadas-spies-collude-energy-sector

secret briefings on a topic as sensitive as foreign interference, which has already given rise to undue scrutiny of specific communities and concerns around anti-Asian racism and Sinophobia, could also result in further marginalization, undue suspicion and racial profiling.

Third, there are important questions of accuracy, transparency, privacy and recourse. By its nature, intelligence is not necessarily based on proven facts, but instead on reports and information coming from various sources, ranging from CSIS surveillance activities to foreign agencies to human sources, and could include concrete information all the way to hearsay. Sometimes intelligence can prove to be wrong, other times we have seen how intelligence – especially unsourced intelligence – can be politically motivated or be the product of questionable or illegal tactics. Despite some prohibitions, there are also cases of intelligence derived through mistreatment and torture being relied on in Canada.

Confidential briefings, even if granted to individuals with security clearance, would result in information being shared behind closed doors. What opportunities would there be to ensure the accuracy of the information being shared? This is particularly concerning if the information being shared is in regard to an individual who is not present and able to defend themselves. Beyond ensuring accuracy, an individual, organization or even entire community that is placed under suspicion would have no opportunity to explain or defend themselves.

There are similarities here to concerns raised by the National Security and Intelligence Review Agency (NSIRA) regarding CSIS threat reduction measures. In its 2021 annual report, NSIRA looked at the involvement of external parties with whom CSIS engaged as part of its TRM activities, which has clear parallels with any new information sharing powers that CSIS may be granted under this proposal.[5] NSIRA reported that:

- CSIS's documentation of the information disclosed to external parties as part of TRMs was inconsistent and, at times, lacked clarity and specificity.
- CSIS did not systematically identify or document the authorities or abilities of external parties to take action, or the plausible adverse impacts of the TRM
- CSIS did not always document the outcomes of a specific TRM, or the actions taken by external parties to reduce a threat.
- CSIS did not appropriately take into account the potential adverse impacts of external parties' actions when considering whether a warrant it required for a TRM authorization.

While CSIS agreed in part with the first three points, they stipulated that they may not have access to the information necessary to provide some of this reporting, with no commitment to finding solutions to better collect and assess this information. They fully disagreed with their responsibility under the fourth point to consider external party activities when deciding whether a warrant application was necessary. Taken together, this paints a concerning picture that CSIS

[5] National Security and Intelligence Review Agency. "Annual Report 2021," 2022. Online: https://nsira-ossnr.gc.ca/wp-content/uploads/AR-2021_EN.pdf

does not believe it is responsible for the broader impact that the information it shares with external parties can have on individuals, including when it may infringe on *Charter* rights.

This is particularly important, because the parties with whom CSIS shares information are not necessarily bound by the same restrictions as the service. For example, private entities are not bound by the *Charter*, nor are they necessarily covered by federal privacy laws, depending on the jurisdiction. The possibility for *Charter*-infringing actions or violations of privacy rights would be significant without appropriately strict guardrails. Expanding information sharing powers, even if restricted to the context of foreign interference, would exacerbate this issue unless there are strict rules as well as a change in approach by CSIS overall.

This leads to our fourth and final concern: that the proposal, as framed, would grant CSIS greater information sharing powers in relation to *all* threats to the security of Canada, and not solely in relation to cases of foreign interference. In the context of a foreign interference consultation, it is difficult to analyze what the impact of such new powers would be when applied to CSIS efforts to counter espionage, sabotage or terrorism - nor is there justification granted in the consultation document as to why it is needed for these other areas. To the contrary, our work on CSIS counter-terrorism activities leads us to conclude that such information sharing powers would pose the same or greater risks as those we have identified above in reference to foreign interference concerns.

Given all this, we would encourage the government to explore other avenues to improve overall information sharing with outside partners regarding foreign interference that do not include legislative changes to the CSIS Act. Alternatively, any future proposal to grant CSIS such powers should be accompanied by detailed information of what other efforts have been made and why new powers for CSIS would be necessary. In this case, the powers should also be narrowly framed as applying to issues of foreign interference, and not to CSIS' overall mandate of addressing threats to the security of Canada.

Issue #2: Whether to implement new judicial authorization authorities tailored to the level of intrusiveness of the techniques

What Do You Think?

1. Should CSIS be able to compel an entity to preserve perishable information when it intends to seek a production order or a warrant to obtain that information?

Amending the *CSIS Act* to allow for the issuing of judicially authorized preservation orders would be acceptable. However, it would be important that there be a clear framework around retention periods, as well as annual reporting on relevant information, including the number of preservation orders issued. We believe that preservation orders would also help to address some

of the concerns around timelines for obtaining warrants, reducing the need to modify the warrant authorization process.

2. Should CSIS be able to compel production of information when it reasonably believes that the information is likely to yield information of importance that is likely to assist in the performance of its duties and functions under sections 12 or 16 of the *CSIS Act*?

We would be largely opposed to new production order powers. We do not believe that enough justification has been given in this consultation document to support a production order power. While a production order may not be as invasive as a search, it has the possibility of placing a burden on the subject of a production order, using up resources and impacting operations.

More importantly, while the proposal is that production orders would remain judicially authorized, we are worried about the vague language used to describe the basis and thresholds for issuing a production order: "reasonably believes," "likely" to yield or assist, and information "of importance." We have seen CSIS greatly expand its data collection and retention powers in the past five years, and the language used here raises distinct concerns that production order powers could lead to unnecessary and broad requests for information without appropriate justification.

Moreover, as noted in the consultation document, CSIS is not a law enforcement agency and is therefore not subject to the same level of transparency and scrutiny. Ministerial oversight, judicial authorization and after-the-fact review are important, but do not compensate for the transparency and scrutiny of, for example, a production order being challenged in open court. While this concern may be most relevant to the question of search warrants, it is also relevant here.

While a party would clearly be informed regarding a production order, such an order would likely be made *ex parte* without challenge. Should the subject of a production order wish to challenge it, they would face the uphill battle of likely not having access to the information justifying the production order, since it would be covered by national security confidentiality. There would also be no public record of the production order, and very likely the subject of the production order would be limited in being allowed to disclose publicly that they were compelled to share information (this has been widely discussed in relation to "transparency reports" from social media platforms, email providers and ISPs).

Were a proposal that addressed our concerns around the thresholds for requesting a production order put forward, we would reconsider it, but as currently presented we would oppose it.

3. Should CSIS be able to conduct a single collection activity, like a one time collection and examination of a USB reasonably believed to contain threat-related information, without having to demonstrate investigative necessity? If yes,

what requirements should CSIS have to meet for seeking different warrant powers?

We are strongly opposed to any new collection powers that would not require demonstrating investigative necessity. We recognize that different investigative methods may carry with them differing levels of intrusiveness, but we do not believe that this justifies a change in CSIS' warrant authorities or to, under any circumstances, eliminate the need for investigative necessity.

While a search of a USB may appear to be limited in nature, the reality is that they can contain vast troves of information (with the upper limit now at 2tb of data and growing). While a warrant may be to obtain a specific piece of information, such a search still opens up access to vast amounts of incidental information. Moreover, what distinction is made between a USB as a storage device and the hard drive of a computer? Or a cell phone (with or without data connection)?

As mentioned above, strict rules around CSIS' warrant frameworks are necessary because the service operates with a high level of secrecy and is not subject to the kind of adversarial challenge and public scrutiny that law enforcement agencies face. In order to ensure effective judicial oversight, stringent requirements are necessary.

CSIS also has demonstrated a troubling history of disdain for the existing warrant process, with one report stating that the culture at CSIS is one of viewing warrants as "burdensome" and a "necessary evil."[6] Courts have also found a consistent history of CSIS either misleading the courts or leaving out key information, violating the duty of candor they owe to the courts.[7] This has not been resolved, and believe demonstrates the need to maintain strict rules around warrant authorizations.

4. In situations where the Minister of Public Safety is unable to authorize the making of a CSIS application for judicial authorization to the Federal Court and where the matter cannot wait, should there be a mechanism to delegate this authority? If yes, who should this authority be delegated to and in what types of situations should this apply to?

We would support this under very specific conditions. The delegation of authority could not be to anyone within CSIS. It could be acceptable to delegate to a deputy or assistant deputy minister, under very clear and exigent circumstances. The Minister would need to review and

[6] Bronskill, J. "CSIS sees warrant process as 'burdensome' and a 'necessary evil': federal review," *The Canadian Press*, 13 Oct. 2020. Online: https://www.cbc.ca/news/politics/csis-warrant-process-independent-review-1.5760390

[7] Bronskill, J. "Court admonishes CSIS once again over duty of candour," *The Canadian Press*, 31 August 2021. Online: https://www.theglobeandmail.com/canada/article-court-admonishes-csis-once-again-over-duty-of-candour/

approve any authorizations as soon as they are once again available, and there would need to be regular reporting to review agencies and to the public.

Issue #3: Whether to close the gap, created by technological evolution, and regain the ability for CSIS to collect, from within Canada, foreign intelligence about foreign states and foreign individuals in Canada

What Do You Think?

1. Should the *CSIS Act* be amended so that CSIS' ability to collect foreign intelligence at the request of Ministers can keep pace with the evolution of technology, which creates digitally borderless information? If so, what should be the limitations?

We would oppose granting CSIS the power to collect foreign intelligence held outside Canada regarding a foreign state or a foreign individual located within Canada.

We recognize that changes in technology mean that information that previously would have been held within Canada may now be held outside of Canada, even if it is accessible from within Canada (for example, over the internet). At face value, it would seem obvious that CSIS should be able to adapt to this change and access this information with prior judicial authorization.

However, it raises several significant concerns. The intent of the limitation of "within Canada" was to avoid

> "aggressive 'covert' and 'offensive' activities abroad," so as "to mitigate the political diplomatic and moral risk of conducting foreign intelligence collection, which [has] the potential to breach foreign international law [and] foreign domestic law and bring disrepute to Canada's international reputation […]."[8]

Granting CSIS the ability to collect foreign intelligence regarding a foreign state that is held outside of Canada, even if all of CSIS' activities take place from within Canada over the internet, would have the effect of completely doing away with the original intent of "within Canada." The state of technology today would mean that vast amounts of information held outside of Canada, but accessible from within Canada, would become fair game for CSIS' s.16 activities. Even if done over the internet, it would still involve the same kind of political, diplomatic and moral risk originally identified; this risk is not limited to "boots on the ground" intelligence gathering activities. Further, in regard to collecting information relating to a foreign state, CSIS would

[8] 2021 FCA 165, para 42

encroach on the Communications Security Establishment's foreign intelligence gathering activities, duplicating mandates and causing confusion.

Regarding collecting intelligence concerning a foreign individual in Canada, it may be possible to argue a narrower scope. For example, being able to access the email account of a foreign individual who is in Canada, but whose email data is held on servers outside of Canada. However, even in this case, it would likely open floodgates of surveillance. An individual may not just access email or social media held on foreign servers, but upload documents to the cloud or foreign governments servers, containing vastly more information. Moreover, it could lead to authorizations to seek information held by third parties abroad related to this foreign individual in Canada, essentially removing all limits on what information CSIS could access, so long as it is done over the internet from within Canada. Beyond vastly broadening the scope of what CSIS could access, it would also once again run the same kind of political, diplomatic and moral risk as noted above.

It is also important not to overlook the fact that there may be other technical solutions that could address these concerns. For example, emails and documents may be accessible within Canada at various stages of transmission and/or may be saved to computers in Canada, while at the same time being held on servers internationally.

We recognize that foreign agents and individuals located in Canada may attempt to take advantage of these limitations by storing information internationally that previously, due to technological limitations, would have only been stored in Canada. A narrow proposal to address this kind of scenario would possibly be more acceptable, but we would require a more concrete proposal in order to address it.

Issue #4: Whether to amend the CSIS Act to enhance CSIS' capacity to capitalize on data analytics to investigate threats in a modern era

What do you think?

We believe it is inappropriate and inadequate to address the question of dataset regime in this consultation. There is a legislatively mandated review of all components of Bill C-59 that is meant to take place this year. The level of information shared, and the level of consultation and debate provided by this consultation are not detailed or thorough enough to make appropriate decisions on any reforms that should be made to the dataset regime. Moreover, any review process should examine the effectiveness of the regime, be backed by data and provide for not just the expansion but also the restriction of powers. This is not present in the current consultation document.

It is worrisome that the government would be attempting to support significant changes to the dataset regime under the auspices of current concerns of "foreign interference", especially given that legislative changes would not be limited to the investigation of foreign interference.

1. How could CSIS increase its ability to collect and use datasets in a timely and relevant manner, while respecting protected *Charter* rights, in a data-driven world?

We do not believe that the evidence presented provides adequate support to justify increasing CSIS' ability to collect and use datasets. There is no evidence presented that the 90 day time limit is actually hindering CSIS in carrying out its mandate. What is the scope of the issue? Have datasets actually been lost? Have there been any circumstances when important intelligence was missed because of the timelines? We do not have the information necessary to evaluate the requests being made. Moreover, while we would not propose that these powers be used more often, section 11.22 (1) allows for non-authorized datasets to be queried under exigent circumstances, if it is necessary to "acquire intelligence of significant importance to national security, the value of which would be diminished or lost if the Service is required to comply with the authorization process under section 11.13 or sections 11.17 and 11.18." If there is important information at risk of being impacted due to the time needed to authorize and query a dataset, there are tools in place.

The safeguards put in place around this regime were established for a very good reason: the dataset regime allows CSIS to expand its collection powers to information that is not strictly necessary for its mandate. The ability to access and retain this kind of information must be strict in order to avoid the further development of mass collection of information regarding individuals who do not pose a threat to the security of Canada. We continue to question the creation of this regime itself, and would hope that the future review will serve to clarify activities carried out under it and, if necessary, to further restrict the program.

2. Should CSIS be able to query or exploit Canadian datasets for section 15 purposes? If so, do you think there should be additional safeguards or limitations in place?

Once again, little information is provided to justify the proposed change. We would require more information as to whether current investigative powers are insufficient in order to justify allowing access to Canadian datasets. Moreover, s.11.2(3) allows for the querying of foreign datasets, granting other avenues of investigation. We therefore oppose the expansion of s.15 to allow the querying of Canadian datasets.

3. Should CSIS be able to share Canadian or foreign datasets with domestic partners who have the lawful authority to collect the type of information contained in the dataset? If so, what safeguards or conditions should be in place, if any?

We strongly oppose granting CSIS the ability to share datasets with domestic partners. These datasets, rightly, are already considered highly sensitive, including in how they are queried. Once a dataset is shared with another entity, it becomes incredibly difficult to control how it is used. Ample powers already exist for CSIS to cooperate with the RCMP, CSE and CBSA, and information disclosure powers exist under the *Security of Canada Information Disclosure Act*. The sharing of information, especially personal information, is incredibly sensitive and must remain closely safeguarded.

4. Should CSIS be allowed to share foreign datasets with foreign partners? If so, what safeguards or conditions should be in place, if any?

We would further oppose the ability to share datasets with foreign entities or partners, given that the concerns expressed in the previous answer are only exponentially amplified by the information being shared with a foreign jurisdiction, completely outside of the Canadian government's control.

We are also troubled that in the final paragraph of this section entirely new modifications to this regime, unrelated to the examples provided, were proposed. These represent significant changes to a very sensitive regime. No such changes should be proposed without an in-depth parliamentary review of the activities of the regime to date.

Issue #5: Whether to introduce a requirement to review the CSIS Act on a regular basis so that CSIS may keep pace with evolving threats

What Do You Think?

1. Should legislation require that CSIS' authorities be regularly reviewed to keep pace with technological advances and Canada's adversaries? If so, how often?
2. Do you have any other views to share regarding the development and possible amendments to the *CSIS Act*?

Yes, there should be regular review. We believe a parliamentary review held every five years would be adequate. However, it is worrisome that the only grounds provided to propose such a review is to keep pace with technological advancements. Regular review should also be an opportunity to account for concerns around rights violations, effectiveness and necessity of CSIS powers, and the possible restriction of mandate or removal of powers, as necessary.

Such a review would need to be supported by robust and public reporting and information sharing, and include feedback from a wide ranges of stakeholders who are provided the opportunity, and commensurate resources, to participate in the review.

Finally, we would emphasize once again the fact that the proposals in this consultation would, if implemented, have wide-ranging impacts across CSIS' activities and would in no way be limited to investigating foreign interference. Before any legislation is brought forward, it would be necessary to consult further and ensure engagement from organizations and experts who may not be working on addressing foreign interference but who are engaged by other aspects of CSIS' mandate.