

For Public Release



Government
— of —
Saskatchewan

**Ministry of Executive Council
Intergovernmental Affairs**

Deputy Minister
300 – 3085 Albert Street
Regina, Canada S4S 0B1

February 16, 2024

Tushara Williams
Deputy Minister of Intergovernmental Affairs
Privy Council Office
Room 1000, 85 Sparks Street
OTTAWA ON K1A 0A3

Dear Tushara Williams:

The Government of Saskatchewan appreciated the consultation meeting between our two orders of government on Friday, January 19, 2024. In follow-up to the consultation with federal officials from the Canadian Security Intelligence Service (CSIS) and the Department of Justice, Saskatchewan is also providing a written submission to comment on the federal government's proposed legislative amendments.

Saskatchewan shares the federal government's concerns regarding foreign interference, including spreading misinformation and deliberately malicious actions. Saskatchewan generally agrees with Public Safety Canada's efforts to counter the following actions:

- threatening, harassing, or intimidating people in Canada or their family and friends abroad because of their political opinions or to shape behaviour;
- attempting to interfere in institutions and processes, such as elections, to advance interests; and
- stealing intellectual property or know-how or imposing market conditions to gain an economic advantage.

Saskatchewan is a highly trade-exposed province. Almost 70% of Saskatchewan's gross domestic product is reliant on exports. Saskatchewan also has a reputation for being open to trade, which could make the province susceptible to being targeted by foreign states and their proxies. Furthermore, Saskatchewan has 23 out of 31 occurrences of critical minerals under Canada's Critical Minerals Strategy, including uranium and rare earth elements. Potential supply chain risks in Saskatchewan could include the theft of industrial secrets or intellectual property, intimidation and blackmail, and industrial sabotage.

... 2

For Public Release

Tushara Williams
Page 2
February 16, 2024

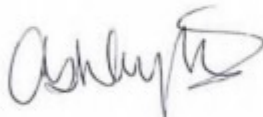
Given Saskatchewan's relative trade-exposure and the importance of our trade infrastructure for getting goods to market, protecting essential infrastructure from sabotage, especially road and rail transport infrastructure, is critical for the province.

Saskatchewan has nine international trade and investment offices located abroad, which could put the Province at risk of retaliatory measures or actions by foreign governments. The inclusion of exemptions in a future Foreign Influence Transparency Registry, including for an individual or organization working on behalf of a foreign government, could be beneficial for Saskatchewan's nine investment and trade offices abroad.

Saskatchewan supports amending the *Canadian Security Intelligence Service Act* to include non-federal partners, such as Provinces and Territories. This amendment would ensure Saskatchewan officials, including those travelling abroad, could be briefed or notified of foreign interference in a more tactical and strategic manner.

Please see the attached appendices for additional comments from the Government of Saskatchewan regarding potential legislative amendments to address foreign interference.

Sincerely,



Ashley Metz
Deputy Minister of Intergovernmental Affairs

Attachments

For Public Release

APPENDIX A

SASKATCHEWAN CANADIAN SECURITY INTELLIGENCE SERVICE ACT RESPONSE

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.	
<p>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?</p>	<p>Saskatchewan supports the release of information outside of the Government of Canada by CSIS in the right context.</p> <p>Information possessed by CSIS can directly impact public safety, conceivably involving terrorism, foreign actors, or other national security issues.</p> <p>Police services of jurisdiction are a primary stakeholder and should be considered as such in information-sharing. Provincial governments also have the fiduciary responsibility to ensure public safety and direct resources to disrupt or prevent threats to public safety.</p>
<p>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?</p>	<p>Information released should be directly or indirectly related to threats to public safety and aid or assist law enforcement or provincial governments to detect, disrupt, or prevent significant public safety threats (i.e., the "need to know principle" with appropriate classification levels).</p> <p>Information shared with provincial entities or law enforcement should not be related to investigations or inquiries into matters that would not be in the mandate of CSIS (i.e. National Security) unless:</p> <ul style="list-style-type: none"> • there is a threat of grievous bodily harm or death to an individual; • it shares details of a significant threat to the public or critical infrastructure; or • it threatens to undermine confidence in the political or democratic processes. <p>Saskatchewan recommends that s.13 of the Act be amended to state that "the Service may provide security assessments to departments of the Government of Canada or the government of a province or any department thereof." This would eliminate the need for CSIS to get the approval of the Minister to disclose security risks to a provincial government and leave it at their own discretion.</p> <p>In the definitions section (s.2) under "threats to the security of Canada," the reference to the "interests of Canada" could be supplemented with the addition of "interests of Canada and its provinces and territories" to emphasize that a threat that affects a province affects the interests of Canada (for example, Saskatchewan's international trade offices).</p> <p>In s.6(4) of the Act, annual reports are to be submitted to the Minister, and language could be added to include Premiers. Further, s.14 should be updated to include any Minister of a provincial government.</p> <p>An amendment to s.19, "authorized disclosure of information," giving the Service discretion to disclose information to provinces and territories as well under s.19(2)(b) "where the information relates to the conduct of the international affairs of Canada..." should be considered. That section currently only authorizes that information to be disclosed to the Minister of Foreign Affairs or designate.</p>

For Public Release

Issue 2: Whether to implement new judicial authorization authorities tailored to the level of intrusiveness of the techniques.	
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?	Yes. This needs to have specific "rules," however. Timelines as to the presenting of a judicial authorization (i.e., production order) by CSIS need to be in place. If CSIS were to "freeze" material from any entity, they need to present that production order within a reasonable period (i.e., 30 days from point of sequestering the information). This will ensure procedural fairness and accountability is maintained by CSIS and that an entity is not "left hanging" as they await the production order or other judicial authorization.
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?	Yes, however, CSIS would be required to obtain authorization (judicial) to obtain that information. That said, in cases where exigent circumstances exist, CSIS should be able to compel information if it is necessary to: <ul style="list-style-type: none"> • prevent an imminent attack or crime; or • address a significant threat to Canada's national security which could result in loss of life or result in significant impacts to critical infrastructure.
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?	Yes, with conditions. CSIS should have to present its rationale and evidence to support any such intrusion, as would any law enforcement agency. However, in cases where a deliberate and illegal activity may occur that poses a significant risk to the national security of Canada, CSIS should be able to conduct such a search. CSIS should have the ability to obtain different authorizations related to different thresholds, depending on what is needed. Using a single warrant authority, appropriate for the most intrusive investigative techniques, negatively impacts the effectiveness of the organization and risks missing potential threats in the initial stages. CSIS should have the ability to obtain the equivalent of a 'production order' in the law enforcement community.
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?	Yes, however, this process should only be used when there are exigent circumstances (i.e., the potential for imminent loss of life or demonstrated high-risk situations with an imminent negative impact to safety and security).
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.	
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?	Yes. National security threats, like cybercrime, are borderless. CSIS' abilities need to be consistent in scope to be effective. CSIS' capabilities need to be aligned with those of the other 5 Eyes countries to ensure restrictive legislation in Canada does not negatively impact the greater intelligence community. Clarification of the proposed Ministers is needed. The Minister of Public Safety is the authority. Does this question suggest that other Ministers in the federal government should be able to direct CSIS in the collection of foreign intelligence? If so, it is necessary to confirm the intent.

For Public Release

Issue 4: Whether to amend the CSIS Act to enhance CSIS' capacity to capitalize on data analytics to investigate threats in a modern era.	
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?	Caution should be applied to any AI-based analytical methods with a stringent review process in place to ensure the accuracy of conclusions.
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?	<p>Yes. The information should be used only for the intended purpose as related to section 15.</p> <p>This query or exploit should be authorized by court unless it is "open source."</p> <p>CSIS should not have the ability to conduct an unauthorized search for this purpose; however, the bar for obtaining a warrant/authorization could be lower since the purpose of s.15 is to provide a security assessment and not for prosecution.</p> <p>Not having this ability negatively impacts the effectiveness of the organization. A time limitation may be appropriate, but it must be longer than 90 days.</p>
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?	<p>Yes. The dataset must not be used for a purpose that is not consistent with the purpose for which it was collected. For example, the dataset should not be used by a domestic organization to commence a civil process against the subject or entities contained in the dataset.</p> <p>Safeguards should include Third Party Rule. The domestic partner cannot further share or use the information provided to them by CSIS without first obtaining permission from CSIS to do so while simultaneously ensuring there's lawful authority to share/use the information.</p>
4. Should CSIS be allowed to share foreign datasets with foreign partners? If so, what safeguards or conditions should be in place, if any?	<p>Yes. The dataset must not be used for a purpose that is not consistent for the purpose in which it is collected. For example, the dataset should not be used by a foreign entity to commence a civil process against the subject or entities contained in the dataset.</p> <p>Release of any foreign datasets should be approved through a standing committee for the expressed purpose.</p> <p>The foreign entity should be made aware and consulted prior to release. Safeguards should include Third Party Rule. The foreign partner cannot further share or use the information provided to them by CSIS without first obtaining permission from CSIS to do so while simultaneously ensuring there's lawful authority to share/use the information.</p>
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.	
1. Should legislation require that CSIS' authorities be regularly reviewed to keep pace with technological advances and Canada's adversaries? If so, how often?	<p>Yes, at an interval of approximately five years.</p> <p>Regular review may not equate to required updates every time. Technology changes quickly.</p>
2. Do you have any other views to share regarding the development and possible amendments to the CSIS Act?	There are several provisions in the Act about regular reporting to the Government of Canada on threats and risks. A modernization of the Act could include the sharing of reports be provided to the provinces as well, as a matter of course. None of these paragraphs in the current Act require disclosure of information to the Canadian government – only permits it. Any additions about disclosure to provinces would likely need to follow suit.

For Public Release

APPENDIX B

SASKATCHEWAN RESPONSE ON FOREIGN INTERFERENCE

Issue 1: Whether to Create New Foreign Interference (FI) Offences.	
<p>1. Should Canada have additional "foreign interference" offences to ensure that we have covered situations like those described in the scenarios? If so, which of the four new offences above do you think would be beneficial?</p>	<p>a. Commission of Indictable offence for a foreign entity b. General FI offence c. Intimidation used offence d. FI in the democratic process offence</p> <p>All four offences have merit and would ease the potential harm caused by FI. Care must be taken to ensure that the offences are 'provable'. Consideration should be undertaken as to who would have primary investigatory or prosecutorial responsibilities. Provinces and territories may not have sufficient resources to take on these types of offences.</p>
<p>2. Instead of creating new offences, would it be better to give the judge the ability to increase the penalty when sentencing an individual if the crime was committed for the benefit of a foreign entity? It may be easier for prosecutors to deal with this issue as an aggravating factor at the sentencing stage, as is done with terrorism offences. This way, if a prosecutor is unable to establish the foreign link, the underlying offence could still be proven. Or should the law do both?</p>	<p>As many avenues as may be available should be utilized to minimize the FI threat. It is noted that not all behaviour is captured by existing offences.</p>
<p>3. What kinds of activities of foreign states are unacceptable in Canada, keeping in mind that Canadian officials are involved in legitimate efforts to advance Canadian interests abroad?</p>	<p>While not a major issue here in Saskatchewan at present, as a jurisdiction with a high degree of trade exposure that is increasing its presence abroad through its international offices our exposure to foreign interference rises accordingly. Activities of concern identified include spreading misinformation, any deliberately malicious actions, and intellectual property theft. There was also general agreement with the actions that Public Safety Canada has outlined:</p> <ul style="list-style-type: none"> • threatening, harassing, or intimidating people in Canada or their family and friends abroad because of their political opinions or to shape behaviour; • attempting to interfere in institutions and processes, such as elections, to advance interests; and • stealing intellectual property or know-how or imposing market conditions to gain an economic advantage.
<p>4. The <i>Security of Information Act</i> already defines the term "foreign entity" as five things: a foreign power; a foreign power and one or more terrorist groups; a group or association of foreign powers; a group or association of foreign powers and one or more terrorist groups; or a person acting at the direction of the first four entities. Do we need to expand what we mean by "foreign entity" in relation to these offences?</p>	<p>What about an individual who is acting without direction but that is committing the offence to bolster a foreign entity? Criminalization in this context might lessen the concern set out in question 2 regarding establishing a foreign link above.</p>

For Public Release

5. Keeping in mind the protections that already exist in the <i>Canada Elections Act</i> and in provincial elections legislation, what sorts of democratic processes, rights and duties warrant protection from foreign interference under the SOIA?	Saskatchewan election legislation speaks to acts that may influence an election but nothing about the act being done for the benefit of a foreign entity. <i>Security of Information Act</i> must fill this gap, and if existing measures do not, they should be emplaced in it.
Issue 2: Whether to amend section 22 of the <i>Security of Information Act</i> to increase the maximum penalty and to have it apply to other offences.	
1. Is a maximum term of imprisonment of five years (as opposed to the existing two years) the appropriate penalty for preparatory acts that fall short of the full act of either espionage, communication of special operational information to a foreign entity or to a terrorist group, and foreign-influenced threats of violence?	Yes. More serious penalties must be reserved for acts that are committed/completed.
2. What is the appropriate maximum penalty for preparatory acts relating to economic espionage (currently two years)?	We would want to avoid giving the accused a right to a jury trial for a preparatory offence and have to keep the maximum penalty to less than five years.
3. Are there other offences in the <i>Security of Information Act</i> to which this provision (preparatory acts offence) should apply?	No.
Issue 3: Whether to Modernize Canada's Sabotage Offence.	
1. a) Should the law of sabotage be updated to ensure it covers modern forms of critical infrastructure such as water, sewage, energy, fuel, communication, and food services? b) Should it be updated to clarify that it covers a broader range of negative impacts on infrastructure? c) Would it be enough to rely on existing offences such as unauthorized use of computer, mischief, use of an explosive or other lethal device against a government or public facility, public transportation, or other infrastructure?	a. These essential services need to be protected, especially in the light of the rise in electronic acts of sabotage. b. If there is to be an expansion of the offence provision at all, it must be broad and flexible enough to be as effective as possible. c. This option will always be available and could be used as companion offences laid in addition to a new offence. They may not be effective enough to do the job expected as they currently exist.
2. Would it be beneficial to give the judge the ability to increase the penalty when sentencing an individual if the crime was committed for the benefit of a foreign entity?	Yes. Aggravating circumstances have come to be considered an important part of the sentencing regime, particularly when they are meant to deter/punish specific conduct.

For Public Release

3. Are the existing exemptions from liability still appropriate? Should other exemptions be considered, like those found in the terrorism provisions of the <i>Criminal Code</i> ? Should there be a requirement to get the consent of the Attorney General to proceed with the offence?	Attorney General consent is a good way to safeguard or mitigate potential issues, but the existing exemptions are adequate. Attorney General consent might be beneficial in special circumstances not necessarily in existence now.
4. a) Would it be appropriate to create an offence to capture possession of a device to commit sabotage? b) Should such an offence require intent to commit sabotage? c) What kinds of devices would be appropriate to include in such an offence?	a. An offence such as possessing break-in instruments in s.351 of the Criminal Code would be effective. b. Not necessarily. Possession of an instrument suitable for the purpose of breaking in, knowing that the instrument has been used or is intended to be used for that purpose as set out in s.351 is a good model to examine/follow. c. We would rely on people who have particular expertise in this area to comment.
Issue 4: Whether to Create a General Secure Administrative Review Proceedings Process under the <i>Canada Evidence Act</i>	
Comments? This is a complex issue and warrants meaningful consultation and discussion amongst stakeholders and the federal and provincial/territorial governments. It would be necessary to ensure procedural/Charter fairness but also that the individual/state's right to protection is balanced. We agree that having a myriad of different regimes for different situations would be difficult to operationalize and encourage discussions that provide as wide a net as possible to capture a process that works in different contexts. The points set out at pages 18 and 19 of the discussion paper are a good starting point for these discussions.	
Issue 5: Whether to introduce reforms to how national security information is protected and used in criminal proceedings	
1. Do you see benefits to the criminal proposals in the investigation and prosecution of foreign interference cases?	<ul style="list-style-type: none"> • Capacity issues would arise should the provincial Crown or court be more involved in these resource/security-intensive types of cases. Federal support would be required if they were. • This concern extends to special counsel that might be appointed to assist in the case. If a provincial judge made the appointment, the province would be hard-pressed to find the resources to pay them to assist the accused. Moreover, even if there were resources, finding counsel to do these cases will be difficult as we already have trouble finding them in other contexts. • With respect to interlocutory appeals, we agree with the suggestion that they should be limited to cases where the Crown would be appealing a decision to disclose information. Where the decision had been made to not disclose information, an appeal should only take place post-trial. • We agree that there should be inclusion of national security, etc. considerations in s. 487.3(2) [sealing order] cases. • We also agree that special procedures be created for a trial court to review and assess sensitive national security information in Garofoli applications.
2. Do the proposals strike the right balance between the protection of information and fundamental rights and freedoms protected by the <i>Charter of Rights and Freedoms</i> ?	While this balance must be maintained, it must be ensured that appropriate resources are provided to ensure both the protection of sensitive information and the accused's Charter rights.

For Public Release

3. Are there other intelligence and evidence-related measures that would assist in this regard?	Other stakeholders or groups may have more expertise and be in a better position to answer this question.
---	---