Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

SECRET // CEO // SOLICITOR-CLIENT PRIVILEGE

DATE: MAY 15 2023

File No.: NS 6210 / PS-039804

MEMORANDUM FOR THE MINISTER OF PUBLIC SAFETY

PROPOSED MINISTERIAL DIRECTION TO THE CANADIAN SECURITY INTELLIGENCE SERVICE ON THREATS TO PARLIAMENTARIANS

(For signature)

ISSUE

s. 39 - Cabinet Confidence

BACKGROUND

Aspect 1: Informing Government on Threats to Parliament

CSIS's core mandate, established at section 12 of the *CSIS Act* is to collect information on threats to the security of Canada and to report to and advise government, which holds responsibility for instituting policies and making decisions to protect national security. It therefore has full authority to disclose analysis of threats to Parliament and parliamentarians to you, as Minister, or to other Government of Canada departments.

There are a number of provisions in current Ministerial Direction that could apply when CSIS identifies threats to Parliament or parliamentarians:

- The Ministerial Direction on Accountability (issued in 2019) specifies that CSIS should consult or inform the Minister "regarding any action on which a Deputy Head would normally involve his or her minister."
- It also requires CSIS to notify the Minister in advance of operational activities for which one of the four risk pillars (operational, legal, reputational, foreign policy) is assessed as high.

Canada

SECRET // CEO // SOLICITOR-CLIENT PRIVILEGE

- The Ministerial Direction on Operations (issued in 2023) requires CSIS to conduct a reputational risk assessment for any CSIS operational activity for intelligence collection related to a Canadian fundamental institution (which would include Parliament); pursuant to the MD on Accountability provision noted above, you would need to be informed if the risk is assessed as high.

There are currently no ministerial directions that would require the Service to inform you in all instances of threats to the security of Canada involving Parliament or parliamentarians. The sharing of intelligence products with you as Minister is a function that is generally covered by the Minister's overall accountability for the Service and CSIS's section 12 mandate.

Aspect 2: Informing Parliamentarians on Threats

CSIS's mandate to advise the federal government, and not third parties, reflects a deliberate choice made when the *CSIS Act* was enacted. The goal is to avoid the risks associated with having an intelligence service using its intelligence to influence society or shape individuals' lives without political accountability. Government departments and police forces are responsible for instituting policies, making decisions, and intervening to prevent threats from manifesting.

The Act therefore only permits CSIS to disclose information outside the federal government in limited circumstances. Parliamentarians – unless they are Ministers of the Crown – are not part of the Government of Canada, irrespective of the party they represent. Circumstances where Parliamentarians and other non-federal government bodies may receive information include the following, which may be relevant in the context of parliamentary security:

- CSIS is able to provide high-level, unclassified information about the general nature of threats to the security of Canada. These may be in the form of a threat overview or "defensive brief," and consist of information on how threats can manifest and be avoided. This information is generally understood as not having been obtained in the performance of CSIS' duties and functions, and can therefore be disclosed outside the Government of Canada.

- CSIS has the authority to disclose information to law enforcement, where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province.

- In limited circumstances, information may be disclosed under CSIS's threat reduction measure (TRM) function. To initiate a TRM, CSIS must have reasonable grounds to believe a particular activity constitutes a threat to the security of Canada. TRMs must be reasonable, proportional, and have as their goal the reduction of that specific and identified threat. To that end, CSIS can only disclose the information needed to reduce that threat. CSIS cannot use the TRM regime to,

for instance, educate individuals about a general problem unless CSIS can reasonably anticipate that such education would result in a reduction of a specific threat.

CSIS is also able to disclose information if the disclosure would enable a subject of investigation to provide new information or corroborate existing information. This is known as the "give to get" practice and is distinguishable from the above circumstances since the purpose of the disclosure is not to provide information, but to collect further information.

There are no specific provisions in Ministerial Direction which speak to whether CSIS should disclose information to Parliamentarians.

CONSIDERATIONS

Role of Minister

There are no significant policy considerations with keeping you informed of CSIS operations, including those related to Parliament or parliamentarians. Keeping you informed of sensitive CSIS operations is important to supporting your accountability for CSIS's activities. Policy considerations would arise, however, if there was a real or perceived degree of influence by you over the conduct of intelligence activities involving parliamentarians. Any perception that you were directing CSIS to collect intelligence against a parliamentarian or disclose intelligence to further political ends could be damaging to the integrity of your office, CSIS, and national security. Any intervention into this space would need to be carefully crafted to avoid creating such a perception now or in the future.

Legislative Gap

The authorities outlined above provide a certain degree of ability for CSIS to disclose information outside the federal government. These authorities generally cover circumstances where the disclosure is general (i.e., defensive, educational briefings) or purposeful (i.e., supporting prosecutions, furthering the collection of information, or implementing threat reduction measures). They do not provide authority for other circumstances, such as where there is a moral or ethical imperative to inform an individual they may be the subject of threat activity, and the disclosure may not result in a specific action that will reduce the threat.

This potential gap has been identified as part of current CSIS and PS analysis of the *CSIS Act* and has been prioritized for policy development. Officials are examining options which could permit CSIS to disclose information in additional circumstances to parliamentarians and other potential targets of foreign interference.

SECRET // CEO // SOLICITOR-CLIENT PRIVILEGE

Information Sharing Considerations

Disclosures of information derived from intelligence raise a number of important policy and operational considerations that must be carefully taken into account when developing policy as well as assessing disclosures for an individual case.

- *Operational security and effectiveness:* Disclosures of information could introduce a risk to CSIS's operational security, including the safety of sources and the effectiveness of intelligence collection methods. Even if information on sources and methods is not directly referenced in the disclosure, third parties may be able to deduce information based on the context or nature of the information. Any retaliatory action, whether directed accurately or inaccurately, could compromise CSIS operations and human sources, as well as the ability of CSIS to recruit further sources.

- *Creation of liabilities:* Once information is disclosed, the federal government does not have control over how the recipient will use the information. If subsequent action is unreasonable (e.g., dismissal of an employee), it could create a real or perceived liability for the federal government for its part in the recipient's actions.

- *Compromise of law enforcement investigations:* It is imperative that the judicial system remains the primary avenue for addressing domestic conduct that harms Canada or Canadians. Disclosures of intelligence that are not properly coordinated and consulted with law enforcement can disrupt their investigations and impair charges and prosecution.

- *Maintaining CSIS's objectivity:* To maintain CSIS's effectiveness, it is important that it is regarded as an impartial and nonpartisan actor. Disclosures of information, particularly in the parliamentary space, could risk creating the perception that these disclosures are related to political discussions and deliberations. For example, if CSIS were to disclose information related to terrorism threats at the same time a terrorism-related bill is before Parliament, it could create the impression these disclosures are intended to influence support for the legislation.

Role of Ministerial Direction

Under the *CSIS Act*, the Director has control and management of CSIS, under the direction of the Minister of Public Safety. Pursuant to section 6(2), the Minister of Public Safety may issue written directions that govern how CSIS exercises its authorities. A copy of each direction must be provided to the National Security and Intelligence Review Agency.

Ministerial Direction cannot grant new authorities not already provided by the *CSIS Act*. However, Direction may guide and constrain how CSIS applies its authorities. Given the considerations that can arise when CSIS is disclosing information, we recommend that Ministerial Direction under the *CSIS Act* s. 39 - Cabinet Confidence

not override case-specific decision making by CSIS, but instead outline the imperatives which should guide CSIS's decision making and require you to be kept informed of key aspects.

PROPOSED MINISTERIAL DIRECTION

Ministerial Direction could be issued to outline principles and expectations to guide CSIS's activities with respect to threats to Parliament and parliamentarians, without overriding case-specific decision making that may be required. This direction could be general, without specifying the specific means for responding to threats or the legal mechanisms for briefing Parliamentarians. As such, it could be issued immediately, while work to address the legislative gap or establish other mechanisms to enhance information sharing occur in tandem. Releasing the direction to the public would provide assurances that there are processes and mechanisms in place to address these threats.

This additional direction could be integrated into the existing Ministerial Direction on Operations. This would continue the practice of having all operational direction to CSIS in one place. However, doing so would present challenges from a transparency and communications perspective. To release the Ministerial Direction on Operations, significant portions would need to be redacted as they relate to sensitive operational matters.

Alternatively, stand alone direction could be issued to CSIS specifically on this subject. This would provide an opportunity to make a clear and complete articulation of the government's approach to this subject without redactions. It would also emphasize the importance of this subject matter.

A proposed, standalone Ministerial Direction on Threats to the Security of Canada Directed at Parliament and Parliamentarians is attached at **TAB A**. It would establish your expectations that:

- Threats to the security of Canada directed at Parliament and parliamentarians receive a degree of attention commensurate with the importance of the institution to Canada's democracy;
- CSIS will pursue all appropriate lawful methods to respond to threats to the security of Canada directed at Parliament and parliamentarians, including the taking of threat reduction measures and disclosing information to the Royal Canadian Mounted Police or other law enforcement body;
- CSIS will seek, wherever possible within the law and while protecting the security of its operations, to ensure that parliamentarians are informed of threat activities directed towards them.

The Direction would also require CSIS to inform you of all instances of threats to the security of Canada directed at Parliament or parliamentarians. When it informs you of

these threats, CSIS would be expected to explain how its response addresses the three expectations outlined above. This means it would be expected to explain how it is investigating the threat, responding to the threat, and informing the affected parliamentarian, where possible within the law.

s. 39 - Cabinet Confidence in reference to a case involving a foreign interference threat, the proposed Ministerial Direction encompasses all threats to the security of Canada, as defined in section 2 of the *CSIS Act*.

The proposed Direction does not specify a threshold for CSIS's information or the severity of the threat. The requirements would be triggered whenever CSIS has sufficient information to determine a threat exists, in accordance with its legal authorities under section 12 of the *CSIS Act*. The proposed Direction also does not specify how the threat must manifest. For example, it would apply to threats that are directed at a parliamentarian through her or his staff, family, or other associates. who does this include?

CSIS's current practice is to inform you of operational activity related to parliamentarians through Issues Management notes and to inform you of threats generally through intelligence reports and assessments. These products are currently circulated to Public Safety for onward distribution. As part of implementing the proposed Direction, the processes for managing these documents could be enhanced to ensure both their tracking and that you personally receive them in a timely manner. We expect that implementation of the Direction will result in an increase in correspondence from CSIS, as well as tips from parliamentarians and others to CSIS, which could have resourcing implications at CSIS and Public Safety Canada.

The proposed Direction applies to the Parliament of Canada only. Questions may arise about the focus, and why other legislatures and potential targets of foreign interference are not included. Similarly, issuing Ministerial Direction on this subject may create an expectation that you issue Ministerial Direction more regularly and responsively to CSIS to address perceived shortcomings in their conduct.

SECRET // CEO // SOLICITOR-CLIENT PRIVILEGE

RECOMMENDATION

It is recommended that you approve the attached Ministerial Direction at **TAB A** by signing below, and by signing the letters to the Director of CSIS (**TAB B**) and the Chair of the National Security and Intelligence Review Agency (**TAB C**).

Should you require additional information, please do not hesitate to contact me or Patrick Boucher, Senior Assistant Deputy Minister, National and Cyber Security, at

Shawn Tupper

Enclosures: (3)

I approve:

The Honourable Marco E. L. Mendicino
Minister of Public Safety

I do not approve:

The Honourable Marco E. L. Mendicino
Minister of Public Safety

Prepared by:

MINISTERIAL DIRECTION ON THREATS TO THE SECURITY OF CANADA DIRECTED AT PARLIAMENT AND PARLIAMENTARIANS

The Parliament of Canada is at the heart of Canada's democracy. As such, it is imperative that all parliamentarians are able to exercise their roles fully and without hindrance or interference from foreign states or hostile actors.

To this end, I expect that threats to the security of Canada directed at Parliament and parliamentarians, including those conducted through their family and staff, receive the highest level of attention from the Canadian Security Intelligence Service (CSIS) in collaboration with the national security and intelligence community. In doing so, I continue to expect that CSIS will at all times respect the *Canadian Charter of Rights and Freedoms* and the rule of law.

Pursuant to subsection 6(2) of the *Canadian Security Intelligence Service Act*, I have issued the following direction to describe my expectations in this regard.

1. CSIS will investigate all threats to the security of Canada that target Parliament and parliamentarians in a manner proportional to the threat and the importance of Parliament to Canada's democracy and national security.

2. When CSIS assesses, in accordance with its mandate, there to be a threat to the security of Canada directed at Parliament or a parliamentarian, it will pursue the appropriate lawful methods in response, including but not limited to the taking of threat reduction measures and disclosures to the Royal Canadian Mounted Police or other law enforcement agencies.

3. CSIS will seek, wherever possible within the law and while protecting the security and integrity of national security and intelligence operations and investigations, to ensure that parliamentarians are informed of threats to the security of Canada directed at them. This may involve direct disclosures, or by working with other bodies, such as Government of Canada departments, the Royal Canadian Mounted Police, or other law enforcement agencies, as the law permits.

4. The Minister of Public Safety will be informed of all instances of threats to the security of Canada directed at Parliament or parliamentarians in a timely manner and with an explanation of how CSIS will implement the above directions.