








Amendments to CSIS Act Disclosure Authorities



Better Equip National Security Partners

National security threats no longer target only the federal government. Foreign interference impacts every level of government – provincial, territorial, municipal, and Indigenous partners – as well as the private sector, academia, and Canada’s diverse communities. Authorizing CSIS to share information more broadly and frequently with persons or entities outside the Government of Canada, can build society-wide resiliency against threats to the security of Canada. Sharing more CSIS information can increase the ability for persons and entities to understand and recognize threats, and to protect their information, assets, and Canada’s interests.

Relevant Authorities Enabling CSIS To Disclose Information

Objective	Current	Amendments
 Investigation and Prosecution of Legal Contraventions	<ul style="list-style-type: none"> May disclose to peace officers to investigate or to Attorney Generals to prosecute someone suspected of breaking the laws of Canada or a province. 	<ul style="list-style-type: none"> ✓ Allows for disclosure to <i>any person</i> with jurisdiction to investigate or to Attorney Generals to prosecute someone suspected of breaking the laws of Canada or a province.
 Build Resiliency	<ul style="list-style-type: none"> CSIS does not have legal ability to share information to build resiliency against threats to the security of Canada, except where it may lead to a concrete reduction of the threat. 	<ul style="list-style-type: none"> ✓ May disclose information to build resiliency. ✓ Cannot disclose personal information of a Canadian citizen, permanent resident or any individual in Canada, or the name of a Canadian entity or corporation incorporated in Canada, unless it is about the recipient of the disclosure. ✓ Information must be provided to the relevant federal department or agency.
 Essential in the Public Interest	<ul style="list-style-type: none"> May disclose to any minister of the Crown or person in the federal public administration, with the approval of the Minister of Public Safety. The Minister must determine that disclosure is essential in the public interest and clearly outweighs any invasion of privacy. Must report the disclosure to the National Security and Intelligence Review Agency. 	<ul style="list-style-type: none"> ✓ May disclose to <i>any person or entity information that could not be released via a resiliency disclosure</i>, with the approval of the Minister of Public Safety. ✓ The Minister must <i>still</i> determine that the disclosure is essential in the public interest and clearly outweighs any invasion of privacy. ✓ Must <i>still</i> report the disclosure to the National Security and Intelligence Review Agency.
 Community Outreach	<ul style="list-style-type: none"> May disclose to any person or entity unclassified and general information. 	<ul style="list-style-type: none"> ➡ Remains unchanged.
 Report to and Advise on Threats	<ul style="list-style-type: none"> Limited to disclosing information to the Federal Government. The Government of Canada is subject to <i>Charter</i> and <i>Privacy Act</i> in its handling of CSIS’ information. 	<ul style="list-style-type: none"> ➡ Remains unchanged.
 Investigate Threats (the “give to get” principle)	<ul style="list-style-type: none"> May disclose to any person or entity but must be reasonably expected to result in the collection of new information by CSIS. 	<ul style="list-style-type: none"> ➡ Remains unchanged.
 Reduce Threats	<ul style="list-style-type: none"> May disclose to any person or entity for the purpose of reducing a threat. CSIS must have reasonable grounds to believe that a particular activity constitutes a threat and the disclosure must be reasonably expected to reduce the threat. Must consult other federal departments or agencies, as appropriate. May require a Federal Court warrant. 	<ul style="list-style-type: none"> ➡ Remains unchanged.

GAPS

- Foreign interference today not only threatens military technology and federal government institutions, but all levels of government and all sectors of society.
- The *CSIS Act* has strict limitations on when, how and to whom CSIS can share information, with the Government of Canada as primary recipient.
- CSIS' inability to share information limits stakeholder's awareness, ability to understand and identify threats, and take protective measures to withstand threats.

IMPACT OF AMENDMENTS

Enable CSIS to disclose information to all investigative officials.

Enable CSIS to disclose more comprehensive information for the purpose of building resilience against threats.

Enable CSIS, with the Minister's approval, to disclose otherwise prohibited personal or private entity information, where it is essential in the public interest.



EXAMPLE: Build Resilience Against Threats

A member of a territorial legislature has been appointed to a territorial cabinet. CSIS has information that a foreign state is interested in using proxies in Canada to exploit the territory for its Arctic access and natural resources. The member's background and advocacy also makes them a more likely target of the foreign state. CSIS would like to provide specific information on foreign interference targeting, and why the member may be a target.

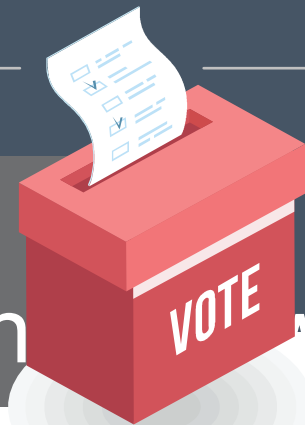
✘ Without amendments

CSIS would only be able to provide an unclassified and general threat briefing. The member is not a part of the Federal Government of Canada, and there is no specific threat that CSIS might reduce by disclosing information to this individual.

✔ With amendments

CSIS would be authorized to share classified information with the member about how the foreign state is using specific tradecraft to target them and why in order to increase the member's understanding, enable him to recognise the threat if it presents itself and build resilience against foreign interference. With the approval of the Minister, CSIS would be able to provide the names of the proxies in Canada.

EXAMPLE: Investigate Contravention



CSIS can only disclose information to recipients for them to investigate alleged contravention of law if that recipient is a peace officer (i.e., a police officer). **With amendments**, CSIS could provide information to municipal, Indigenous, provincial and territorial elections officials who are not peace officers but have jurisdiction to investigate alleged corrupt practice under their elections legislation.



Amendments to the CSIS Act



Amendments to the 40 year old, pre-digital era *CSIS Act* will better equip CSIS to ensure the safety, security and prosperity of Canada and all Canadians. The amendments respond to urgent gaps in CSIS' authorities that are limiting its ability to protect Canada and all Canadians in an increasingly complex threat environment fuelled by technology.

All amendments were developed to ensure that CSIS activities comply with the *Canadian Charter of Rights and Freedoms* and continue to have robust oversight by Parliament, the courts, and the Minister.

The Amendments
will Better
Enable CSIS to:



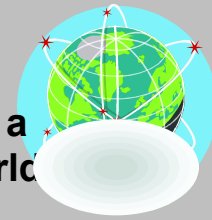
1

Equip National
Security Partners



2

Operate in a
Digital World



3

Respond to
Evolving Threats

Disclosure



Current state: CSIS lacks authority to disclose information to partners outside the Government of Canada to build resiliency against threats.

Amendments will enable CSIS to:

- ✓ Disclose information to build resiliency against threats.
- ✓ With the approval of the Minister of Public Safety, to disclose personal information when it is essential in the public interest and clearly outweighs privacy invasion.
- ✓ Disclose information to any person with jurisdiction to investigate someone suspected of breaking the laws of Canada or a province.

Rigorous safeguards, including the limit on disclosing personal information and Canadian corporate names will ensure privacy is protected. Disclosures in the public interest must be reported to the National Security and Intelligence Review Agency.

Example: CSIS could rely on the new resiliency disclosure authority to provide comprehensive information to the premier of a province or Indigenous government or diaspora community who may be a likely target of the foreign interference activities of the proxies of a foreign state. This would enable them to better recognise the threat if it presents itself and build resiliency against foreign interference.

Warrants and Orders



Current state: The absence of a range of judicial authorizations impedes, delays, and at times halts, national security investigations. This can diminish CSIS' ability to protect all Canadians.

Amendments will enable CSIS to:

- ✓ Conduct a single collection activity (i.e., single use warrant to examine a USB key).
- ✓ Compel a third party to keep information without deleting it, to allow time for CSIS to seek a production order or warrant.
- ✓ Compel a third party to produce information.
- ✓ Remove a thing previously installed with permission (removal warrant).
- ✓ Require assistance for the single use and removal warrants.

Federal Court approval is *still* required for all warrants and orders, with review and robust oversight by the Minister and the National Security and Intelligence Review Agency.

Example: If a foreign interference threat actor is transiting through a Canadian airport, CSIS may only have a small window to examine their smartphone, making it nearly impossible to demonstrate investigative necessity. The single-use warrant would be the right tool for a one-time examination of their electronic device while the threat actor is in transit.

Dataset



Datasets are groups or collections of information about a common topic that are stored in electronic form. They can vary in size from a few entries to billions of records.

Current state: Advances in digital technology are giving threat actors the advantage and causing CSIS to lag behind partners and adversaries alike.

Amendments will:

- ✓ Increase overall timelines. For example, from 90 to 180 days to decrypt, translate and assess datasets (evaluate) before seeking permission to retain.
- ✓ Clarify that datasets support CSIS' core mandate.
- ✓ Enable sharing of datasets, with appropriate approvals.
- ✓ Enable use of Canadian datasets for Government and immigration security screening investigations.
- ✓ Enable broader use of data analytics in exigent (i.e., urgent) circumstances.
- ✓ Allow foreign datasets to be treated as Canadian datasets, which are subject to the most stringent safeguards.

All of the safeguards remain, including the critical role of the Intelligence Commissioner.

Example: CSIS could have a dataset of individuals in Canada who have lived in a country known to engage in foreign interference, and which happens to contain past educational information for each person. CSIS could query and exploit this dataset for the purpose of a screening investigation for a government clearance. In doing so, it could learn that the individual studied at a university associated with a foreign military, which is relevant but was not disclosed in the application.

Foreign Intelligence



Current state: The current borderless nature of information has reduced CSIS' visibility on the activities of foreign states or foreign individuals within Canada's borders.

Amendments would:

- ✓ Close the technical gap so CSIS can collect information from within Canada that is located outside Canada, when the information is about the activities of foreign individuals in Canada.
- ✓ Enable CSIS to continue collection from within Canada when a foreign individual is temporarily outside Canada.

Collection of foreign intelligence will continue to be at the request of the Minister of National Defence or Foreign Affairs and can only target non-Canadians, in Canada.

Statutory Review



- ✓ Require the *CSIS Act* to be reviewed by Parliament every five years, ensuring CSIS can continue to protect and remain accountable to Canada and all Canadians.

Technical Amendment



- ✓ Make a technical amendment to clarify that, with emergency designations, employees may be justified in committing or directing another person to commit acts or omissions that would otherwise constitute offences.



CSIS is accountable to Parliament and all Canadians to ensure respect for the rights and freedoms of all Canadians and people in Canada.


- Attorney General of Canada
- Federal Court
- Minister of Public Safety
- Canadian Public
- Auditor General
- Intelligence Commissioner
- Privacy Commissioner
- Information Commissioner
- Commissioner of Official Languages
- National Security and Intelligence Review Agency
- National Security and Intelligence Committee of Parliamentarians

Amendments to CSIS Act Warrant Authorities



Having a greater variety of investigative tools can enable CSIS to use the right tool, at the right time, to protect all Canadians. It can also ultimately be less intrusive overall because CSIS will *not* have to use multiple non-warranted techniques for extended periods of time, and because it will focus CSIS' investigations to rule people out so CSIS can quickly focus on the right threat actors.

Federal Court approval is required for any activity that is more than minimally intrusive and the Court may impose any terms or conditions it deems appropriate.

	 Federal Court Approval	 Investigative Necessity Approval	 Ministerial Approval	 Authorizes	 Duration
Current s. 21 Warrant	✓	✓	✓	<ul style="list-style-type: none"> All investigative techniques, including interception. Can use repeatedly. Ongoing and future collection. 	Up To a Year.
Preservation Order	✓	✗	✗ <small>Notification as soon as feasible</small>	<ul style="list-style-type: none"> Requires a third party to preserve (<i>not</i> destroy or delete) information or thing. Does <i>not</i> authorize any collection by CSIS. 	90 days.
Production Order	✓	✗	✓	<ul style="list-style-type: none"> Requires a third party to provide information to CSIS that is in their possession or control. Does <i>not</i> authorize CSIS to deploy <i>any</i> investigative techniques. Allows for judicial review. 	Determined by the Court.
Single-Use Warrant	✓	✗	✓	<ul style="list-style-type: none"> Single, one-off investigative technique. Does <i>not</i> authorize the interception of communications. Does <i>not</i> authorize ongoing collection of any kind. 	120 days or when the single activity is completed, whichever comes first.
Amendments to Existing Removal Warrant	✓	✗	✓	<ul style="list-style-type: none"> Amended to address the removal of a thing previously installed by CSIS with permission. Amended to include the reasonable grounds to believe threshold (previously none). Does <i>not</i> authorize any collection by CSIS. 	Determined by the Court.
Amendments to Existing Assistance Order	✓	✗	✓ <small>Tied to authorizations that require Ministerial approval</small>	<ul style="list-style-type: none"> <i>Not</i> an authorization by itself. Requires a third party to provide assistance to CSIS in executing existing warrant. Amended to include the new single use warrant and the removal warrant. 	Tied to the underlying authorization (120 days up to one year).



GAPS

- The toolkit in the *CSIS Act* is old and predates the internet.
- The amendments, while new to the *CSIS Act*, are *not* new tools; they are modelled on powers routinely relied on by Canadian law enforcement and intelligence agencies in other democracies.
- The threshold for accessing these tools is still high. Safeguards have been built in and are strong. The amendments were developed with a view to ensure *no Charter* or other rights are negatively affected.

GAPS BEING ADDRESSED

CSIS *cannot* currently compel the preservation of perishable information.

CSIS does *not* have an appropriate tool to compel the production of information.

CSIS does *not* currently have a tool to perform a single collection activity to focus investigations.

EXAMPLE: Preservation and production order



CSIS' current warrant authority requires an application for a warrant demonstrate other investigative techniques:

- Have been tried and failed or why they are unlikely to succeed;
- Are impractical in urgent circumstances, or
- That information of importance will not be obtained without the warrant.

These elements are referred to as 'investigative necessity' requirements.

Most Internet service providers have policies requiring routine deletion of information. A **preservation order** from the Federal Court would authorize CSIS to require a provider to retain account information for an individual operating on behalf of a foreign state and observed to be posting mis- and disinformation about a candidate for mayor. This would prevent deletion.

Afterwards, CSIS would have to seek a **production order** from the Federal Court to require the internet provider to provide the account information to CSIS.

Production orders could also allow CSIS to acquire:

- subscriber information;
- call, transaction or financial records;
- stored communications and phone or computer backups.



EXAMPLE: Single use warrant

If there was a FI threat actor who is transiting through a Canadian airport, CSIS may only have a small window to examine their electronic device (eg. Smartphone) because they may be in Canada for only a few hours.

Currently, CSIS would have to establish investigative necessity to seek a warrant. This would be nearly impossible given the very short window to first use other investigative techniques such as interviews or surveillance. The single-use warrant would be the right tool for a one-time examination of their electronic device while the threat actor is in transit.

