








# 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 – as well as the private sector, academia, and Canada’s diverse communities. Bill C-70, *An Act respecting countering foreign interference*, amended the *Canadian Security Intelligence Service Act (CSIS Act)* to better detect, disrupt and protect against foreign interference. The amendments authorize the Canadian Security Intelligence Service (CSIS) to share information more broadly and frequently with persons or entities outside the Government of Canada, which will build society-wide resilience against threats to the security of Canada. Sharing more CSIS information will increase the ability for persons and entities to understand and recognize threats, and to protect their information, assets, as well as Canada’s interests.

## Relevant Authorities Enabling CSIS To Disclose Information

| Objective  | Former Authorities   | With Amendments  |
|--|--|--|
|  <b>Investigation and Prosecution of Legal Contraventions</b> | <ul style="list-style-type: none"><li>May disclose to peace officers to investigate or to attorneys general to prosecute someone suspected of breaking the laws of Canada or a province.</li></ul>   | <ul style="list-style-type: none"><li>Allows for disclosure to <i>any person</i> with jurisdiction to investigate or to attorneys general to prosecute someone suspected of breaking the laws of Canada or a province.</li></ul>   |
|  <b>Build Resiliency</b>                                      | <ul style="list-style-type: none"><li>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.</li></ul>   | <ul style="list-style-type: none"><li>May disclose information to build resiliency.</li><li>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.</li><li>Information must be provided to the relevant federal department or agency.</li></ul>   |
|  <b>Essential in the Public Interest</b>                      | <ul style="list-style-type: none"><li>May disclose to any minister of the Crown or person in the federal public administration, with the approval of the Minister of Public Safety.</li><li>The Minister must determine that disclosure is essential in the public interest and clearly outweighs any invasion of privacy.</li><li>Must report the disclosure to the National Security and Intelligence Review Agency.</li></ul> | <ul style="list-style-type: none"><li>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.</li><li>The Minister must <i>still</i> determine that the disclosure is essential in the public interest and clearly outweighs any invasion of privacy.</li><li>Must <i>still</i> report the disclosure to the National Security and Intelligence Review Agency.</li></ul> |
|  <b>Community Outreach</b>                                    | <ul style="list-style-type: none"><li>May disclose to any person or entity unclassified and general information.</li></ul>   | <ul style="list-style-type: none"><li>Remains unchanged.</li></ul>   |
|  <b>Report to and Advise on Threats</b>                       | <ul style="list-style-type: none"><li>Limited to disclosing information to the Government of Canada.</li><li>The Government of Canada is subject to the <i>Charter</i> and <i>Privacy Act</i> in its handling of CSIS’ information.</li></ul>  | <ul style="list-style-type: none"><li>Remains unchanged.</li></ul>   |
|  <b>Investigate Threats</b><br>(the “give to get” principle)  | <ul style="list-style-type: none"><li>May disclose to any person or entity but must be reasonably expected to result in the collection of new information by CSIS.</li></ul>   | <ul style="list-style-type: none"><li>Remains unchanged.</li></ul>   |
|  <b>Reduce Threats</b>  | <ul style="list-style-type: none"><li>May disclose to any person or entity for the purpose of reducing a threat.</li><li>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.</li><li>Must consult other federal departments or agencies, as appropriate.</li><li>May require a Federal Court warrant.</li></ul>    | <ul style="list-style-type: none"><li>Remains unchanged.</li></ul>   |

# Gaps Filled

- 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* had strict limitations on when, how and to whom CSIS could share information, with the Government of Canada as primary recipient.
- CSIS’ former inability to share information limited 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 resiliency 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 Resiliency 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.



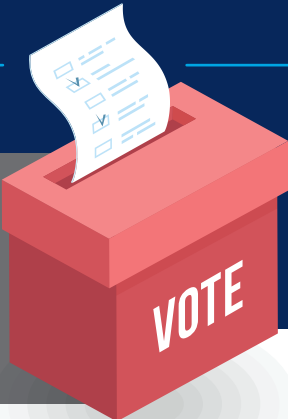
### ✗ Before amendments

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

### ✓ After 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 of Law



Before amendments, CSIS could 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). **After amendments**, CSIS could provide information to Indigenous, municipal, provincial and territorial elections officials who are not peace officers but have jurisdiction to investigate alleged corrupt practice under their elections legislation.