Amendments to *CSIS Act* Warrant Authorities

Bill C-70, *An Act respecting countering foreign interference*, amended the *Canadian Security Intelligence Service Act* (*CSIS Act*), providing the Canadian Security Intelligence Service (CSIS) a greater variety of investigative tools enabling CSIS to use the right tool, at the right time, to protect all Canadians. These new tools can ultimately be less intrusive overall because CSIS will not have to use multiple non-warranted techniques for extended periods of time, allowing CSIS to focus its investigations to rule people out so that CSIS can quickly focus on the right threat actors.

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

	Federal Court Approval	Investigative Necessity	Ministerial Approval	Authorizes	Duration
Existing s. 21 Warrant	✓	✓	✓	• All investigative techniques, including interception. • Can use repeatedly. • Ongoing and future collection.	Up To a Year.
New Preservation Order	✓	✗	✗ Notification as soon as feasible	• Requires a third party to preserve (*not* destroy or delete) information or thing. • Does *not* authorize any collection by CSIS.	90 days.
New Production Order	✓	✗	✓	• Requires a third party to provide information to CSIS that is in their possession or control. • Does *not* authorize CSIS to deploy *any* investigative techniques. • Allows for judicial review.	Determined by the Court.
New Single-Use Warrant	✓	✗	✓	• Single, one-off investigative technique. • Does *not* authorize the interception of communications. • Does *not* authorize ongoing collection of any kind.	120 days or when the single activity is completed, whichever comes first.
Amendments to Existing Removal Warrant	✓	✗	✓	• 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 *not* authorize any collection by CSIS.	Determined by the Court.
Amendments to Existing Assistance Order	✓	✗	✓ Tied to authorizations that require Ministerial approval	• *Not* an authorization by itself. • Requires a third party to provide assistance to CSIS in executing existing s. 21 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 FILLED

- The toolkit in the *CSIS Act* was old and predated 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 ensure *no Charter* or other rights are negatively affected.

IMPACT OF AMENDMENTS	Enable CSIS to compel the preservation of perishable information.	Enable CSIS to compel the production of information.	Enable CSIS to perform a single collection activity to focus investigations.

EXAMPLE: Preservation and production order

Most Internet service providers have policies requiring routine deletion of information. A **preservation order** from the Federal Court could 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 could seek a **production order** from the Federal Court to require the Internet provider to provide the account information to CSIS.

Investigative Necessity

CSIS' existing s. 21 warrant authority requires that an application for a warrant demonstrates that 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.

Production orders could also allow CSIS to acquire:

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

EXAMPLE: Single-use warrant

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

With CSIS' existing s. 21 warrant, 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 new single-use warrant could be used for a one-time examination of their electronic device while the threat actor is in transit.