Bill C-26: Joint Submission to the House of Commons Standing Committee on Public Safety and National Security

Canadian Civil Liberties Association
Canadian Constitution Foundation
International Civil Liberties Monitoring Group
Ligue des Droits et Libertés
National Council of Canadian Muslims
OpenMedia
Privacy and Access Council of Canada
Prof Andrew Clement
Dr Brenda McPhail

Executive Summary

Dear Committee Members,

As organisations and individuals committed to upholding civil liberties, we share the Government of Canada's objective of strengthening cybersecurity, and supporting the public and private sectors, and individual Canadians, to better protect themselves against cyberattacks and other cyber threats.

However, Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* ("Bill C-26" hereafter), raises several areas of serious concern from the perspective of civil liberties, privacy, and democratic freedoms.

In a 28 September, 2022 joint letter to former Public Safety Minister Marco Mendicino, we set out detailed concerns about Bill C-26 across the following areas:

- Opens to the door to new surveillance obligations
- Permits secret termination of essential services
- Offers no guardrails to constrain abuse
- Undermines individual and organisational privacy
- Secretly undermines accountability and due process
- Allows unknowable orders that trump public regulation
- Allows secret evidence in Court, contrary to principles of fundamental justice and open courts
- Provides power without oversight or accountability for the Communications Security Establishment (CSE)

We were encouraged to hear our concerns reflected by Members of Parliament from across the political spectrum throughout Bill C-26's 2nd Reading debate.

We draw Committee members' attention to the enclosed Recommended Remedies that address civil liberties concerns, and ensure Bill C-26 delivers strong cybersecurity for everyone in Canada, while ensuring accountability and upholding Canadians' rights.

Our Recommendations are divided into five key areas of concern:

1. Restraining Ministerial Powers
2. Protecting Confidential Personal and Business Information
3. Maximizing Transparency
4. Allowing Special Advocates to Protect the Public Interest
5. Enhancing accountability for the CSE

Under each of these headings is a short summary of our concerns, and Recommended Remedies.

The Recommended Remedies are a mix of legislative and narrative recommendations, and stem primarily from the findings Dr. Christopher Parsons set out in his report *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act*, published by the Citizen Lab at the University of Toronto in October 2022, and which was referred to multiple times by MPs during the 2nd Reading debate.

Although the scope of Dr. Parsons' report was limited to the *Telecommunications Act* amendments in Bill C-26, we have, where appropriate, mirrored his recommendations for the *Critical Cyber Systems Protection Act (*CCSPA*)*.

We believe that our recommendations systematically address the concerns raised by MPs, and provide a basis for moving forward swiftly with this legislation once Parliament returns. The recommendations also enable Bill C-26 to fulfil its stated objectives of bolstering cyber security across the financial, telecommunications, energy, legal and transportation sectors; prohibiting Canadian companies from using products and services from high-risk suppliers; and helping organizations and individuals better prepare, prevent, and respond to cyber incidents.

We look forward to discussing these Recommended Remedies further with Committee Members when scrutiny of Bill C-26 commences this fall.

An online copy of this document is available at https://tinyurl.com/C26BriefSECU

Bill C-26: Recommended Remedies

Table of Contents

Remedy 1: Restrain Ministerial Powers

Summary of the problem:

Several of our concerns stem from the extensive powers Bill C-26 grants the government in s. 15.2 of the *Telecommunications Act* amendments, and in s. 20 of the *CCSPA*, including that it:

- **Opens the door to new surveillance obligations:** Bill C-26 empowers the government to secretly order telecom providers *"to do anything or refrain from doing anything."* This opens the door to imposing surveillance obligations on private companies, and to other risks such as weakened encryption standards — something the public has long rejected as inconsistent with our privacy rights.

- **Risks the termination of essential services:** Under Bill C-26, the government can bar a person or company from being able to receive specific services, and bar any company from offering these services to others, by secret government order. This opens the door to Canadian companies or individuals being cut off from essential services without explanation. Bill C-26 fails to set out any explicit regime, such as an independent regulator with robust powers, for dealing with the collateral impacts of government Security Orders.

- **Contains no guardrails to constrain abuse:** Bill C-26 lacks mandatory proportionality, privacy, or equity assessments, or other guardrails, to constrain abuse of the new powers it grants the government — powers accompanied by steep fines or even imprisonment for non-compliance. These orders apply both to telecommunications companies, and to a wide range of other federally-regulated companies and agencies designated under the *Critical Cyber Systems Protection Act (CCSPA)*. Prosecutions can be launched in respect of alleged violations of Security Orders which happened up to three years in the past.

Recommended Remedies:

Recommendation 1.1 — Orders in Council and Ministerial Orders must be necessary, proportionate, and reasonable:

(This recommendation is based on Dr. Parsons' Recommendation 1)

The Ministerial powers proposed in Bill C-26 go far beyond what is necessary to secure the telecommunications sector. Bill C-26 provides powers that the Minister could use to access personal information, direct telecoms to spy on Canadians, and cut Canadians off from the internet, among other interventionist powers.

Adding a proportionality test and the obligation to consult with experts will help ensure the Minister does not use trivial problems to justify disproportionately extreme or intrusive actions. The legislation should be amended to impose further conditions surrounding the specific circumstances under which the government may exercise its powers:

Telecommunications Act **Original Text:**	**Telecommunications Act** **Recommended Remedies:**

15.2 (1) If, in the Minister's opinion, it is necessary to do so to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption, the Minister may, by order and after consultation with the Minister of Public Safety and Emergency Preparedness, 15.5 (3)(c) the disclosure is necessary, in the Minister's opinion, to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption. 15.7 (1) Any information collected or obtained under this Act, other than information designated as confidential under subsection 15.5(1), may be disclosed by the Minister under an agreement, a memorandum of understanding or an arrangement in writing between the Government of Canada and the government of a province or of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, if the Minister believes that the information may be relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state, including against the threat of interference, manipulation or disruption.	15.2 (1) If, in the Minister's opinion, it is necessary to do so to secure the Canadian telecommunications system, ~~including~~ against the threat of interference, manipulation or disruption, the Minister may, by order and after consultation with the Minister of Public Safety and Emergency Preparedness, 15.5 (3)(c) the disclosure is necessary, in the Minister's opinion, to secure the Canadian telecommunications system, ~~including~~ against the threat of interference, manipulation or disruption. 15.7 (1) Any information collected or obtained under this Act, other than information designated as confidential under subsection 15.5(1), may be disclosed by the Minister under an agreement, a memorandum of understanding or an arrangement in writing between the Government of Canada and the government of a province or of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, if the Minister believes that the information may be relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state, ~~including~~ against the threat of interference, manipulation or disruption.
15.2 (2) The Minister may, by order, direct a telecommunications service provider to do anything or refrain from doing anything — other than a thing specified in subsection (1) or 15.1(1) — that is specified in the order and that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption. In the order, the Minister may, among other things,	15.2 (2) The Minister may, by order, direct a telecommunications service provider to do anything or refrain from doing anything — other than a thing specified in subsection (1) or 15.1(1) — that is specified in the order and that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, ~~including~~ against the threat of interference, manipulation or disruption. In the order, the Minister may, ~~among other things,~~
	Add after s.15.2(2): "(3) No order may be issued under subsections (1) or (2) unless there are reasonable grounds to believe that the order is necessary and the scope and substance of the order is proportionate and reasonable in the circumstances. (4) Prior to the issuance of an order under subsections (1) or (2), the Minister shall consult with the Minister of Public Safety and Emergency

	Preparedness and a prescribed body of industry experts about the nature and content of the order. The timing and content requirements of the consultation shall be determined by the Minister, having regard to the nature and urgency of the circumstances."

CCSPA **Original Text:**	**CCSPA** **Recommended Remedies:**
20 (1) The Governor in Council may, by order, direct any designated operator or class of operators to comply with any measure set out in the direction for the purpose of protecting a critical cyber system.	"20 (1) The Governor in Council may, by order, direct any designated operator or class of operators to comply with any measure set out in the direction for the purpose of protecting a critical cyber system against a material threat."
	Add after s.20 (1): "(2) No order may be issued under subsection (1) unless there are reasonable grounds to believe the order is necessary and the scope and substance of the order is proportionate and reasonable in the circumstances. (3) Prior to the issuance of an order under subsection (1), the Governor in Council shall consult with the Minister of Public Safety and Emergency Preparedness and a prescribed body of industry experts about the nature and content of the order. The timing and content requirements of the consultation shall be determined by the Governor in Council, having regard to the nature and urgency of the circumstances."

Recommendation 1.2 — The standards that can be imposed must be defined:

(This recommendation is based on Dr. Parsons' Recommendation 5)

The legislation should be amended such that it is clear what kinds of standards are within and outside of the scope of the legislation. It should be made explicit that an order or regulation compelling the adoption of particular standards cannot be used to deliberately or incidentally compromise the confidentiality, integrity, or availability of a telecommunications facility, telecommunications service, or transmission facility.

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedy:**

15.2 (3)(l) require that a telecommunications service provider implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities.	15.2 (3)(l) require that a telecommunications service provider implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities. An order or regulation compelling the adoption of particular standards must not be used to deliberately or incidentally compromise the confidentiality, integrity, or availability of a telecommunications facility, telecommunications service, or transmission facility.

Additionally, we note, especially for MPs, the following recommendations from the learned Dr. Parsons:

- **Parsons Recommendation 24: Clarity Should Exist Across Legislation:** The government should clarify how the envisioned threats under the draft legislation ("including against the threat of interference, manipulation or disruption.") compares to the specific acts denoted in s. 27(2) of the *Communications Security Establishment Act* (CSE Act) ("mischief, unauthorized use or disruption"), with the goal of explaining whether the Telecommunications Act reforms would expand, contract, or address the same classes of acts as considered in the CSE Act.

- **Parsons Recommendation 25: Explicit Definitions Should Be Included In the Legislation or Else Publicly Promulgated:** The legislation should be amended to provide either explicit definitions for "interference," "manipulation," and "disruption," or reference definitions found in specific other Acts, or it should require the government to publicly promulgate these definitions and any updates that are subsequently made to the definitions outside of the legislation.

Finally, we note that our Recommendation 3.6, which would ensure that all regulations issued under Bill C-26 would be accessible to the Standing Joint Committee on the Scrutiny of Regulations, is also relevant to this section. We cover this recommendation in the Maximizing Transparency section below.

Remedy 2: Protect Confidential Personal & Business Information

Summary of the problem:

Bill C-26 **undermines privacy** by empowering the government to collect broad categories of information from designated operators, at any time and subject to any conditions, or none at all. This may enable the government to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations.

Recommended Remedies:

Recommendation 2.1 — Relief should be available if Government mishandles personal or de-identified information:

(This recommendation is based on Dr. Parsons' Recommendation 14)

The legislation should be amended to enable individuals to seek relief if the government or a party to whom the government has disclosed their personal or de-identified information negligently or unintentionally loses control of that information and where that loss of control materially affects the individual.

RECOMMENDED REMEDY - Telecommunications Act:

1. Add after s. 15.7 (2) the words:

   Private Right of Action
   (3) Any person who is affected by an act or omission by the government, or by a person or entity to whom the government has disclosed their confidential information, has a cause of action for damages for loss or injury suffered as a result of the contravention if
   (a) The government, or the person or entity to whom the government has disclosed their confidential information, loses control of that information, and
   (b) That loss of control materially affects or prejudices that person.

   Limitation period or prescription
   (4) An action must not be brought later than two years after the day on which the person becomes aware of the loss of control over the confidential information.

   Court of competent jurisdiction
   (5) An action referred to in subsection (3) may be brought in the Federal Court or a superior court of a province.

RECOMMENDED REMEDY - CCSPA:

1. Add after s. 27 (2) the words:

   Private Right of Action
   (3) Any person who is affected by an act or omission by the government, or by a person or entity to whom the government has disclosed their confidential information, has a cause of action for damages for loss or injury suffered as a result of the contravention if
   (c) The government, or the person or entity to whom the government has disclosed their confidential information, loses control of that information, and
   (d) That loss of control materially affects or prejudices that person.

Limitation period or prescription
(4) An action must not be brought later than two years after the day on which the person becomes aware of the loss of control over the confidential information.

Court of competent jurisdiction
(5) An action referred to in subsection (3) may be brought in the Federal Court or a superior court of a province.

Recommendation 2.2 — Data retention periods should be attached to telecommunications providers' data and to foreign disclosures of information:

(This recommendation is based on Dr. Parsons' Recommendations 17 and 18)

The legislation should be amended to make clear that information obtained from telecommunications providers, or operators designated by the CCSPA, will be retained only for as long as necessary to make, amend, or revoke an order under section 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a) of the Telecommunications Act, or Section 20 of the CCSPA, or to verify the compliance or prevent non-compliance with such an order or regulation. Retention periods should be communicated to telecommunications providers from which the Minister has collected information.

The legislation should also be amended to require that the government attach data retention and deletion clauses in agreements or memoranda of understanding that are entered into with foreign governments or agencies.

RECOMMENDED REMEDY - Telecommunications Act:

1. Add after s. 15.7 (2) the words:

   "**Data Retention Periods**
   (3) Any information collected or obtained under this Act will be retained only for as long as necessary to make, amend, or revoke an order under section 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a), or to verify the compliance or prevent non-compliance with such an order or regulation.

   (4) Retention periods should be communicated to the person from whom the Minister, or person designated by the Minister under section 15.4, has collected the information.

   (5) Any agreement, memorandum of understanding, or arrangement in writing between the Government of Canada and the government of a foreign state, an international organization of states or an international organization established by the governments of states, must include data retention and deletion clauses to ensure it is retained only for as long as is necessary for the purposes set out in subsection (1)."

RECOMMENDED REMEDY - CCSPA:

1. Add after s. 26(2) the words:

   "**Data Retention Periods**

(3) Any information collected or obtained under this Act will be retained only for as long as necessary to make, amend, or revoke an order under section 20, or to verify the compliance or prevent non-compliance with such an order or regulation.

(4) Retention periods should be communicated to the person from whom the Governor in Council has collected the information.

(5) Any agreement, memorandum of understanding, or arrangement in writing between the Government of Canada and the government of a foreign state, an international organization of states or an international organization established by the governments of states, must include data retention and deletion clauses to ensure it is retained only for as long as is necessary for the purposes set out in subsection (1)."

Recommendation 2.3 — Telecommunication providers & designated operators should be informed which foreign parties receive their information:

(This recommendation is based on Dr. Parsons' Recommendation 19)

The legislation should be amended such that telecommunications providers, or operators designated under the CCSPA, are explicitly informed of when and, if so, to whom information may be disclosed when the receiving party is a foreign state, agency, organization, or party:

RECOMMENDED REMEDY - Telecommunications Act:

2. Add after s. 15.7 (1) the words:

   "(2) Persons from whom the Minister, or person designated by the Minister, has collected information under section 15.4 shall be informed when, and to whom, such information has been disclosed when the receiving party is a foreign state, an international organization of states or an international organization established by the governments of states."

RECOMMENDED REMEDY - CCSPA:

1. Add after s. 27(1) the words:

   "(2) Persons from whom the Minister, or person designated by the Minister, a responsible minister or a regulator has collected information under section 26(1) shall be informed when, and to whom, such information has been disclosed when the receiving party is a foreign state, or an international organization established by the governments of foreign states."

Recommendation 2.4 — Legislation should delimit the conditions wherein a private organization's information can be disclosed:

(This recommendation is based on Dr. Parsons' Recommendation 20)

Parliament should restrict the conditions under which the Minister may disclose a private organizations' information:

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
15.7 (1) Any information collected or obtained under this Act, other than information designated as confidential under subsection 15.5(1), may be disclosed by the Minister under an agreement, a memorandum of understanding or an arrangement in writing between the Government of Canada and the government of a province or of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, if the Minister believes that the information may be relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state, including against the threat of interference, manipulation or disruption.	15.7 (1) Any information collected or obtained under this Act, other than information designated as confidential under subsection 15.5(1), ~~may~~ will only be disclosed by the Minister under an agreement, a memorandum of understanding or an arrangement in writing between the Government of Canada and the government of a province or of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, if the Minister believes that the information ~~may~~ is or will be be relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state, ~~including~~ against the threat of interference, manipulation or disruption.

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**
27 (2)(b) the Minister, the responsible minister or the regulator, as the case may be, is satisfied that the information will be treated in a confidential manner and not be further disclosed without their express consent.	27 (2)(b) the Minister, the responsible minister or the regulator, as the case may be, is satisfied that the information will be treated in a confidential manner and not be further disclosed without their express consent; and (c) the Minister, the responsible minister, or the regulator believes the information is or will be relevant to the protection of critical cyber systems."

Recommendation 2.5 — Define personal information as confidential information, and prohibit disclosure of personal or de-identified information to foreign organizations:

(This recommendation is based on Dr. Parsons' Recommendations 28 & 30)

The legislation should be amended to make clear that all personal information and de-identified information that is disclosed by telecommunications providers, or providers designated under the CCSPA, is classified as confidential information, and may not be disclosed to foreign governments or organizations.

RECOMMENDED REMEDY - Telecommunications Act:

1. Add after s. 15.5 (1)(c) the words:
   (d) "information that is personal or de-identified."

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**
26 (1) Subject to subsection (2), a person must not knowingly disclose confidential information or allow it to be disclosed to any agency, body or other person or allow any other agency, body or other person to have access to the information, except if	26 (1) Subject to subsection (2), a person must not knowingly disclose confidential information, including information that is personal or de-identified, or allow it to be disclosed to any agency, body or other person or allow any other agency, body or other person to have access to the information, except if

Recommendation 2.6 — Prior judicial approval to obtain personal or de-identified information:

(This recommendation is based on Dr. Parsons' Recommendation 29)

The Bill, as worded, would allow the Minister to share confidential information with anyone. This is wrong and should be subject to checks and balances to ensure the Minister does not disclose injurious information without first seeking an order from the Federal Court.

The legislation should be amended such that before the government can compel a telecommunications provider to disclose personal or de-identified information, it must first obtain a relevant judicial order from the Federal Court, where the information is to be used exclusively for the purposes of making, amending, or revoking an order under s. 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a), or of verifying compliance or preventing noncompliance with such an order or regulation.

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
15.5 (3)(c) the disclosure is necessary, in the Minister's opinion, to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption.	15.5 (3)(c) on application to the Federal Court, a judge is satisfied by information on oath that there are reasonable grounds to believe that the disclosure is necessary~~, in the Minister's opinion,~~ to secure the Canadian telecommunications system, ~~including~~ against the threat of interference, manipulation or disruption. 15.5 (3)(d) demonstrable exigent circumstances exist which, in the Minister's opinion, make the disclosure necessary to secure the Canadian telecommunications system against an urgent

	threat of interference, manipulation, or disruption. In such circumstances, the Minister shall within 30 days make an application to the Federal Court, and provide information under oath justifying the disclosure.

Additionally, we note Recommended Remedies to impose a duty of confidentiality on regulators with respect to records they obtain under the powers set out in sections 32, 41, 50, 59, 68 & 78 of the CCSPA:

RECOMMENDED REMEDY - CCSPA:

1. Add after s. 32 (3):
   "Confidentiality
   (4) The Superintendent shall ensure the confidentiality of any document, record or cyber system removed pursuant to paragraph (2)(f) and any copy made pursuant to paragraph 2(f)."

2. Add after s. 41 (3):
   "Confidentiality
   (4) The inspector shall ensure the confidentiality of any document, record or cyber system removed pursuant to paragraph (2)(f) and any copy made pursuant to paragraph 2(f)."

3. Add after s. 50 (3):
   "Confidentiality
   (4) The person designated under subsection 49(1) shall ensure the confidentiality of any document, record or cyber system removed pursuant to paragraph (2)(f) and any copy made pursuant to paragraph 2(f)."

4. Add after s. 59 (3):
   "Confidentiality
   (4) The person designated under subsection 58(1) shall ensure the confidentiality of any document, record or cyber system removed pursuant to paragraph (2)(f) and any copy made pursuant to paragraph 2(f)."

5. Add after s. 68 (3):
   "Confidentiality
   (4) The inspection officer shall ensure the confidentiality of any document, record or cyber system removed pursuant to paragraph (2)(f) and any copy made pursuant to paragraph 2(f)."

6. Add after s. 78 (3):
   "Confidentiality
   (4) The Minister of Transport shall ensure the confidentiality of any document, record or cyber system removed pursuant to paragraph (2)(f) and any copy made pursuant to paragraph 2(f)."

Finally, we also note that our Recommendation 5.1, which would ensure that information obtained from Telecommunications Providers is only used for Cybersecurity and Information Assurance activities, is relevant to this section. We cover this recommendation in the 'Enhanced Accountability for the CSE' section below.

Remedy 3: Maximize Transparency

Summary of the Problem:

- **Secrecy undermines accountability and due process:** Bill C-26 enables the government to shroud its orders in secrecy, with no mandatory public reporting requirements. While there is an understandable need for some degree of confidentiality in this sphere, the public needs to have a sense of how these powers are being exercised, how often, and to what effect, if decision-makers are to be held to account. Individuals and services collaterally impacted by Bill C-26 must also be given an opportunity to challenge Security Orders.

- **Unknowable orders trump public regulation:** Bill C-26 tilts the balance so far toward secrecy, that its orders and regulations may take precedence over decisions previously issued by regulatory agencies, risking confusion where such regulatory decisions are public while the Security Orders are not. This threatens the integrity and accessibility of Canada's regulatory frameworks, and renders the security-related rules currently in effect unknowable for members of the public.

Recommended Remedies:

Recommendation 3.1 — Address the absence of transparency and accountability provisions:

(This recommendation is based on section 2.2 of Dr. Parsons' Report)

Bill C-26 allows the government to keep secret any order made to telecommunications providers. While there are certainly situations where secrecy might be warranted, it should not be the default. Requiring an order from the Federal Court acts as a check and balance against government overreach, and will be an effective way to ensure the government is not hiding disproportionately intrusive actions:

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
Non-disclosure 15.1 (2) The order may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person.	**Non-disclosure** 15.1 (2) ~~The order may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person.~~ The Governor in Council may bring an application to the Federal Court for an order prohibiting the disclosure of some or all of the contents of the order issued under subsection (1). The Federal Court may make an order to that effect where it is satisfied that there are reasonable grounds to believe that the disclosure of some or all of the order would be injurious to international relations, national defence or national security or endanger the safety of any person.

Non-disclosure 15.2 (3) An order made under subsection (1) or (2) may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person.	**Non-disclosure** 15.2 (3) ~~An order made under subsection (1) or (2) may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person.~~ The Minister may bring an application to the Federal Court for an order prohibiting the disclosure of some or all of the contents of the order issued under subsection (1) or (2). The Federal Court may make an order to that effect where it is satisfied that there are reasonable grounds to believe that the disclosure of some or all of the order would be injurious to international relations, national defence or national security or endanger the safety of any person.

A similar situation applies to the CCSPA, which allows the government to keep secret any order made to designated operators. Again, while there are certainly situations in which secrecy may be appropriate, opacity should not be the default. These Recommended Remedies will permit designated operators to disclose the existence of a direction, but not its content, except to the extent necessary to comply with the direction:

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**
Prohibition against disclosure 24 Every designated operator that is subject to a cyber security direction is prohibited from disclosing, or allowing to be disclosed, the fact that a cyber security direction was issued and the content of that direction, except in accordance with section 25.	**Prohibition against disclosure** 24 Every designated operator that is subject to a cyber security direction is prohibited from disclosing, or allowing to be disclosed, ~~the fact that a cyber security direction was issued and~~ the content of that direction, except in accordance with section 25.
Disclosure — when allowed 25 (1) A designated operator that is subject to a cyber security direction may disclose the fact that the direction was issued and its content only to the extent necessary to comply with the direction.	**Disclosure — when allowed** 25 (1) A designated operator that is subject to a cyber security direction may disclose ~~the fact that the direction was issued and~~ its content only to the extent necessary to comply with the direction.

Recommendation 3.2 — Orders Should Appear in the *Canada Gazette:*

(This recommendation is based on Dr. Parsons' Recommendation 6)

The legislation should be amended to require that orders be published in the *Canada Gazette* within 180 days of being issued or within 90 days of an order being implemented, based on whichever condition is met first:

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
15.1 (4) Any order made under subsection (1) must be published in the *Canada Gazette*, unless the Governor in Council directs otherwise in the order.	15.1 (4) Any order made under subsection (1) must be published in the *Canada Gazette*, ~~unless the Governor in Council directs otherwise in the order.~~ within 180 days of the order being issued or within 90 days of the order being implemented, based on whichever condition is met first.
15.2 (5) Any order made under subsection (1) or (2) must be published in the *Canada Gazette*, unless the Minister directs otherwise in the order.	15.2 (5) Any order made under subsection (1) or (2) must be published in the *Canada Gazette*, ~~unless the Minister directs otherwise in the order.~~ within 180 days of the order being issued or within 90 days of the order being implemented, based on whichever condition is met first.

Recommendation 3.3 — The Minister should be compelled to table reports pertaining to Orders and Regulations:

(This recommendation is based on Dr. Parsons' Recommendation 7)

The legislation should be amended such that the Minister (or Governor in Council for the CCSPA) is required to table to Parliament an annual report. If the Minister fails to table such reports, the Minister should be required to appear before a parliamentary committee to explain this failure and provide a time frame within which the report will be tabled:

RECOMMENDED REMEDY - Telecommunications Act:

1. Add after s. 15.2(7) the words:

   Reporting
   (8) The Minister shall table to Parliament an annual report stating:

   (a) the number of orders and regulations that have been made under subsection (1) or (2) in the immediately preceding year;
   (b) the number of orders and regulations under subsection (1) or (2) that have been revoked in the immediately preceding year;
   (c) the kinds of orders or regulations that have been made under subsection (1) or (2) in the immediately preceding year;
   (d) the number of applications that have been made to the Federal Court seeking to prohibit disclosure of an order, and the number of applications granted;
   (e) the number of telecommunications providers that have received orders and regulations made under subsection (1) or (2) in the immediately preceding year;
   (f) the number of telecommunications providers that have partially complied with orders and regulations made under subsection (1) or (2) in the immediately preceding year;
   (g) the number of telecommunications providers that have completely complied with orders and regulations made under subsection (1) or (2) in the immediately preceding year; and
   (h) a narrative discussion of the necessity, proportionality, reasonableness, and utility of the order-making powers set out in subsection (1) or (2)

(9) If the Minister fails to table such a report, the Minister shall be required to appear before a parliamentary committee to explain this failure and provide a time frame within which the report will be tabled.

RECOMMENDED REMEDY - CCSPA:

1. Add after s. 146 the words:

   Reporting
   (1) This report shall outline:

   (a) the number of directions made under section 20 in the immediately preceding year;
   (b) the number of directions under section 20 that have been revoked in the immediately preceding year;
   (c) the kinds of directions made under section 20 in the immediately preceding year;
   (d) the number of designated operators that have received directions made under section 20 in the immediately preceding year;
   (e) the number of designated operators that have partially complied with directions made under section 20 in the immediately preceding year;
   (f) the number of designated operators that have completely complied with directions made under section 20 in the immediately preceding year; and
   (g) a narrative discussion of the necessity, proportionality, reasonableness, and utility of the order-making powers set out in section 20

Recommendation 3.4 — Gags should be time-limited:

(This recommendation is based on Dr. Parsons' Recommendation 8)

The legislation should be amended to include a specific period of time after which an order or regulation is received, or following the time of compliance with an order or regulation, that a telecommunications provider, or operator designated by the CCSPA, may publicize that it received and/or entered into compliance with an order, regulation, or direction:

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
Non-disclosure 15.2 (3) An order made under subsection (1) or (2) may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person.	**Non-disclosure** 15.2 (3) An order made under subsection (1) or (2) may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person, prior to its publication in the *Canada Gazette*."

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**

Prohibition against disclosure 24 Every designated operator that is subject to a cyber security direction is prohibited from disclosing, or allowing to be disclosed, the fact that a cyber security direction was issued and the content of that direction, except in accordance with section 25.	**Prohibition against disclosure** 24 Every designated operator that is subject to a cyber security direction is prohibited from disclosing, or allowing to be disclosed, the fact that a cyber security direction was issued and the content of that direction, except in accordance with section 25, or until 180 days have passed since the cyber security direction was issued.

Recommendation 3.5 — The CRTC should indicate when orders override parts of CRTC Decisions; and an Annual Report should include the number of times Government Orders or Regulations prevail over CRTC Decisions:

(This recommendation is based on Dr. Parsons' Recommendations 9 & 10)

The legislation should be amended to, at a minimum, require that the Canadian Radio-television and Telecommunications Commission (CRTC) post a public notice attached to any of its decisions where there is a contradiction between its decision and an Order in Council or Ministerial Order or regulation that has prevailed over part of a CRTC decision.

The legislation should also require the government to annually disclose the number of times it has issued orders or regulations that prevailed in the case of an inconsistency between a given order or regulation and a CRTC decision, as well as denote which CRTC decision(s) were affected.

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
Conflict 15.2 (6) In the event of any inconsistency between an order made under subsection (1) or (2) and a decision of the Commission made under this Act or another order made, or any authorization issued, by the Minister under this Act or the *Radiocommunication Act*, the order made under subsection (1) or (2), as the case may be, prevails to the extent of the inconsistency.	**Conflict** 15.2 (6) In the event of any inconsistency between an order made under subsection (1) or (2) and a decision of the Commission made under this Act or another order made, or any authorization issued, by the Minister under this Act or the Radiocommunication Act~~, the order made under subsection (1) or (2), as the case may be, prevails to the extent of the inconsistency.~~ (a) the order made under subsection (1) or (2), as the case may be, prevails to the extent of the inconsistency; (b) the Commission shall post a public notice attached to the decision(s) affected by the inconsistency; and (c) the Minister shall publish an annual report stating the number of times orders made under subsection (1) or (2) prevailed over Commission decisions.
Conflict	**Conflict**

15.8 (2) In the event of any inconsistency between a regulation made under paragraph (1)(a) and a decision of the Commission made under this Act or an order made or an authorization issued by the Minister under this Act or the *Radiocommunication Act*, the regulation prevails to the extent of the inconsistency.	15.8 (2) In the event of any inconsistency between a regulation made under paragraph (1)(a) and a decision of the Commission made under this Act or an order made or an authorization issued by the Minister under this Act or the *Radiocommunication Act*~~, the regulation prevails to the extent of the inconsistency.~~ a) the regulation prevails to the extent of the inconsistency; b) the Commission shall post a public notice attached to the decision(s) affected by the inconsistency; and c) the Minister shall publish an annual report stating the number of times regulations made under paragraph 1(a) prevailed over Commission decisions.

Recommendation 3.6 — All regulations should be accessible to the Standing Joint Committee for the Scrutiny of Regulations:

(This recommendation is based on Dr. Parsons' Recommendation 11)

The legislation should be amended such that the Standing Joint Committee for the Scrutiny of Regulations is able to obtain, assess, and render a public verdict on any regulations that are promulgated under the proposed draft reforms to the Telecommunications Act and CCSPA. The Committee should also be empowered to obtain, assess, and render a public verdict on regulations pertaining to the *Telecommunications Act* and that are modified pursuant to s. 18 of the *Statutory Instruments Act*.

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
Statutory Instruments Act 15.3 (3) The *Statutory Instruments Act* does not apply to an order made under section 15.1 or 15.2.	***Statutory Instruments Act*** 15.3 (3) The *Statutory Instruments Act* ~~does not apply~~ applies to ~~an~~ all orders made under section 15.1 or 15.2.

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**
Exemption from *Statutory Instruments Act* 22 (1) An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 22 (1) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act.*~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).

Exemption from *Statutory Instruments Act* 34 (2) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 34 (2) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 36 (3) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 36 (3) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 43 (2) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 43 (2) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 45 (3) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 45 (3) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 52 (2) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 52 (2) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 54 (3) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 54 (3) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 61 (2) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 61 (2) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).

Exemption from *Statutory Instruments Act* 63 (3) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 63 (3) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 70 (3) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 70 (3) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 73 (4) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 73 (4) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 81 (2) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 81 (2) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).
Exemption from *Statutory Instruments Act* 82 (3) An order made under subsection (1) is exempt from the application of the *Statutory Instruments Act*.	~~**Exemption from**~~ ***Statutory Instruments Act*** 82 (3) ~~An order made under section 20 is exempt from the application of sections 3, 5 and 11 of the *Statutory Instruments Act*.~~ The *Statutory Instruments Act* applies to all orders made under subsection (1).

Remedy 4: Allow Special Advocates to Protect the Public Interest

Summary of the Problem:

Secret evidence in Court: Even if Security Orders are subjected to judicial review, Bill C-26 could restrict applicants' access to evidence. The legislation does not include any consideration of security-cleared advocates to be appointed on applicants' behalf, as happens in other national security cases. While such provisions are an imperfect solution for due process, they do provide at least a minimal level of protection for applicants' rights. C-26 even empowers judges to make rulings based on secret evidence that is not provided, even in summary form, to applicants or their legal team. It also places the onus on the target of Security Orders to bring legal proceedings, with the associated cost burden.

Recommended Remedies:

Recommendation 4.1 — Create a Special Advocate to enable evidence to be tested in a court of law without being disclosed to outside parties:

(This recommendation builds on the proposal set out in Dr. Parsons' Recommendation 12)

As currently drafted, Bill C-26 allows the Minister to bring secret evidence to secret hearings and mandate that no one see the evidence. That flies in the face of judicial transparency. To properly balance the need for secrecy with the need for judicial transparency, these Recommended Remedies borrow from the Immigration Act and Refugee Protection Act and create a "special advocate", a government-selected lawyer with top secret security clearance who can challenge the evidence the government produces in secret. This way the evidence would be able to be tested in a court of law without being disclosed to any outside parties:

Telecommunications Act Original Text	**Telecommunications Act Recommended Remedies:**
Rules 15.9 (1) The following rules apply to judicial review proceedings in respect of an order made under section 15.1 or 15.2 or a regulation made under paragraph 15.8(1)(a):	**Rules** 15.9 (1) The following rules apply to judicial review proceedings in respect of an order made under section 15.1 or 15.2 or a regulation made under paragraph 15.8(1)(a): (a) the judge shall appoint a person from a list established by the Minister to act as a special advocate in the proceeding after hearing representations from the applicant and the Minister and after giving particular consideration and weight to the preferences of the applicant;
15.9 (1)(b) the judge must ensure the confidentiality of the evidence and other information provided by the Minister if, in the judge's opinion, its disclosure would be injurious to international relations, national defence or	15.9 (1)(b) the judge must ensure the confidentiality of the evidence and other information provided by the Minister if, in the judge's opinion, its disclosure would be injurious to international relations, national defence or

national security or endanger the safety of any person;	national security or endanger the safety of any person; (i) on the request of the Minister, the judge may exempt the Minister from the obligation to provide the special advocate with a copy of information if the judge is satisfied that the information does not enable the applicant to be reasonably informed of the case made by the Minister; (ii) for the purpose of deciding whether to grant an exemption under paragraph (i), the judge may ask the special advocate to make submissions and may communicate with the special advocate to the extent required to enable the special advocate to make the submissions, if the judge is of the opinion that considerations of fairness and natural justice require it;
	Add to the end of s.15.9(1): "(i) the judge may receive into evidence anything that, in the judge's opinion, is reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence; and (j) the judge shall not base a decision on information that the Minister is exempted from providing to the special advocate, shall ensure the confidentiality of that information and shall return it to the Minister."
	After s.15.9(3) add: "**Special advocate's role** **(4)** A special advocate's role is to protect the interests of the applicant in a proceeding when information or other evidence is heard in the absence of the public and of the applicant and their counsel. **Special advocate's responsibilities** **(5)** A special advocate may challenge: (i) the Minister's claim that the disclosure of information or other evidence would be injurious to international relations, national defence or national security or endanger the

	safety of any person; and (ii) the relevance, reliability and sufficiency of information or other evidence that is provided by the Minister and is not disclosed to the applicant and their counsel, and the weight to be given to it. **Obligation to provide information** **(6)** Subject to paragraph 15.9(1)(b)(i), the Minister shall, within a period set by the judge, provide the special advocate with a copy of the information and other evidence that is relevant to the case made by the Minister that has been filed with the Federal Court, but that is not disclosed to the applicant and their counsel."

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**
Judicial review — rules 145 (1) The following rules apply to judicial review proceedings in respect of the issuance of a cyber security direction under section 20:	**Judicial review — rules** 145 (1) The following rules apply to judicial review proceedings in respect of the issuance of a cyber security direction under section 20: (a) the judge shall appoint a person from a list established by the Minister to act as a special advocate in the proceeding after hearing representations from the applicant and the Minister and after giving particular consideration and weight to the preferences of the applicant;
145 (1) (b) the judge must ensure the confidentiality of the evidence and other information provided by the Minister if, in the judge's opinion, its disclosure would be injurious to international relations, national defence or national security or endanger the safety of any person;	145 (1) (b) the judge must ensure the confidentiality of the evidence and other information provided by the Minister if, in the judge's opinion, its disclosure would be injurious to international relations, national defence or national security or endanger the safety of any person; (i) on the request of the Minister, the judge may exempt the Minister from the obligation to provide the special advocate with a copy of information if the judge is satisfied that the information does not enable the applicant to be reasonably informed of the case made by the Minister;

	(ii) for the purpose of deciding whether to grant an exemption under paragraph (i), the judge may ask the special advocate to make submissions and may communicate with the special advocate to the extent required to enable the special advocate to make the submissions, if the judge is of the opinion that considerations of fairness and natural justice require it;"
	Add to the end of s.145 (1): (i) the judge may receive into evidence anything that, in the judge's opinion, is reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence; and (j) the judge shall not base a decision on information that the Minister is exempted from providing to the special advocate, shall ensure the confidentiality of that information and shall return it to the Minister
	After s. 145 (3), add: **"Special advocate's role** (4) A special advocate's role is to protect the interests of the applicant in a proceeding when information or other evidence is heard in the absence of the public and of the applicant and their counsel. **Special advocate's responsibilities** (5) A special advocate may challenge (i) the Minister's claim that the disclosure of information or other evidence would be injurious to international relations, national defence or national security or endanger the safety of any person; and (ii) the relevance, reliability and sufficiency of information or other evidence that is provided by the Minister and is not disclosed to the applicant and their counsel, and the weight to be given to it. **Obligation to provide information** (6) Subject to paragraph 145(1)(c)(i), the

	Minister shall, within a period set by the judge, provide the special advocate with a copy of the information and other evidence that is relevant to the case made by the Minister that has been filed with the Federal Court, but that is not disclosed to the applicant and their counsel.”

Remedy 5: Enhance accountability for the Communications Security Establishment

Summary of the Problem:

Power without accountability for the Communications Security Establishment: The CCSPA would let the Communications Security Establishment (CSE) — Canada's signal intelligence and cybersecurity agency — obtain and analyze security-related data from companies that Canadians entrust with their most sensitive personal information. This would include federally-regulated banks and credit unions, telecommunications and energy providers, and even some transit agencies. The CSE's use of this information is not constrained to the cybersecurity aspect of its mandate, and any uses would be largely subject to after-the-fact review rather than real-time oversight, resulting in a significant deficit in democratic accountability.

Recommended Remedies:

Recommendation 5.1 — Information obtained should only be used for cybersecurity and information assurance activities:

(This recommendation is based on Dr. Parsons' Recommendation 16)

The legislation should be amended to restrict government agencies to exclusively use information obtained from telecommunications providers under Bill C-26 for cybersecurity and information assurance activities. Information should not be permitted to be used for the purposes of signal intelligence and foreign intelligence activities, cross-department assistance unrelated to cyber-security, or active or defensive cyber operations. These restrictions should apply to all agencies, including but not limited to those under the purview of the Minister of Public Safety and Emergency Preparedness.

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
1. ADD after s.15.6 the words: "15.6 (2) Any information shared in accordance with section 15.6 can only be used by the recipient person for purposes exclusively relevant to securing the Canadian telecommunications system against the threat of interference, manipulation or disruption."	

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**
Guidance from Communications Security Establishment 16 An appropriate regulator may provide to the Communications Security Establishment any information, including any confidential information, respecting a designated operator's cyber security program or any steps taken under	**Guidance from Communications Security Establishment** 16 An appropriate regulator may provide to the Communications Security Establishment any information, including any confidential information, respecting a designated operator's cyber security program or any steps taken under

section 15, for the purpose of requesting advice, guidance or services from the Communications Security Establishment in accordance with the mandate of the Communications Security Establishment, in respect of the exercise of the appropriate regulator's powers or the performance of its duties and functions under this Act.	section 15, for the purpose of requesting advice, guidance or services from the Communications Security Establishment in accordance with the cybersecurity and information assurance mandate of the Communications Security Establishment as set out in section 17 of the *CSE Act*, in respect of the exercise of the appropriate regulator's powers or the performance of its duties and functions under this Act.
2. ADD after s.23 the words: "23.1 Any information shared in accordance with section 23 can only be used by the recipient person for the purposes set out in section 5."	
Right to disclose information preserved 26 (2) Nothing in this section precludes a person from disclosing confidential information to a law enforcement agency or the Canadian Security Intelligence Service if the disclosure of the information is otherwise lawful.	**Right to disclose information preserved** 26 (2) Nothing in this section precludes a person from disclosing confidential information to a law enforcement agency or the Canadian Security Intelligence Service if the disclosure of the information is otherwise lawful. **Restriction - use:** 26 (3) Information disclosed subject to subsections (1) or (2) must be used exclusively for purposes related to the protection of vital services, vital systems or critical cyber systems.

Additionally, we note that the National Security and Intelligence Review Agency (NSIRA) has, for two straight years (2020, 2021), reported problems getting access from the CSE to information that the watchdog uses to confirm the lawfulness of the CSE's activities. Fixing this accountability gap is essential to build public confidence that the CSE is operating within the bounds of the law. In this regard, MPs might wish to consider steps, such as imposing an obligation on all reviewed agencies, including the CSE, to publicly provide comments on compliance or expected compliance to requests from their review bodies within a fixed timeframe. MPs might also wish to consider that all orders issued under s.15.2 of the *Telecommunications Act* or s.20 of the *CCSPA* are accessible to NSIRA.

We also note, especially for MPs, the following recommendations from the learned Dr. Parsons:

- **Parsons Recommendation 24: Clarity Should Exist Across Legislation:** The government should clarify how the envisioned threats under the draft legislation ("including against the threat of interference, manipulation or disruption.") compares to the specific acts denoted in s. 27(2) of the CSE Act ("mischief, unauthorized use or disruption"), with the goal of explaining whether the Telecommunications Act reforms would expand, contract, or address the same classes of acts as considered in the CSE Act.

- **Parsons Recommendation 25: Explicit Definitions Should Be Included In the Legislation or Else Publicly Promulgated:** The legislation should be amended to provide either explicit definitions for "interference," "manipulation," and "disruption," or make clear that the definitions are found in specific other Acts, or it should require the government to publicly promulgate these definitions and any updates that are subsequently made to the definitions outside of the legislation.

References & Resources:

Key resources:

- Full text of Bill C-26
- C-26 Legislative Summary (Library of Parliament)
- Civil Society Joint Letter (PDF) (aussi en français)
- Civil Society Media Release (aussi en français)
- Citizen Lab / Dr Chris Parsons report: Cybersecurity will not thrive in darkness (PDF)

Media coverage:

- Canadian Press: Federal cybersecurity bill threatens privacy, transparency, civil society groups say (Jim Bronskill)
- News Forum - Canadian Justice: Bill C-26, Cybersecurity & Civil Liberties (Host Christine Van Geyn interviews Dr Brenda McPhail (CCLA) and OpenMedia's Rosa Addario)
- CTV News Power Play: Interview with Dr Chris Parsons
- Canadian Press: Liberal cybersecurity bill a 'bad law' that must be amended, research report warns (Jim Bronskill)
- IT World Canada: Proposed telecom cybersecurity law gives Canadian government too much secret power: Researcher
- Policy Options: Don't give CSE more powers until it submits to effective review (Dr Chris Parsons)
- Hill Times: Canadians' privacy could take a serious hit this coming legislative session (Ken Rubin)
- CTV News / Canadian Press: Mendicino open to working with MPs to 'improve' much-criticized cybersecurity bill
- Toronto Star (Op-Ed by OpenMedia): MPs must say no to agency request for powers to spy on your bank and travel records