LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PRELIMINARY VERSION

UNEDITED

The preliminary version of this legislative summary is made available to parliamentarians, parliamentary staff and the public to ensure timely access to the information, research and analysis needed to study the bill in question. The official version of the legislative summary, which may differ from this unedited version, will replace this document on the Parliament of Canada website.

Legislative Summary

BILL C-8: AN ACT RESPECTING CYBER SECURITY, AMENDING THE TELECOMMUNICATIONS ACT AND MAKING CONSEQUENTIAL AMENDMENTS TO OTHER ACTS

45-1-C8-E

20 April 2026

Revised by Sabrina Charland

This publication is based on a previous Library of Parliament publication by Jed Chong, Khamla Heminthavong and Holly Porteous.

Library and Research Services

PRELIMINARY VERSION
UNEDITED

AUTHORSHIP

20 April 2026	Sabrina Charland
28 August 2025	Sabrina Charland
6 October 2022	Jed Chong, Khamla Heminthavong and Holly Porteous

ABOUT THIS PUBLICATION

Library of Parliament legislative summaries summarize bills currently before Parliament and provide background information about them in an objective and impartial manner. They are prepared by Library and Research Services, which carries out research for and provides information and analysis to parliamentarians, Senate and House of Commons committees and parliamentary associations. Legislative summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

For clarity of exposition, the legislative proposals set out in the bill described in this legislative summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the Senate and House of Commons and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent and come into force.

Any substantive changes to this Library of Parliament legislative summary that have been made since the preceding issue are indicated in **bold print**.

© Library of Parliament, Ottawa, Canada, 2026

Legislative Summary of Bill C-8
(Preliminary version)

45-1-C8-E

Ce document est également publié en français.

PRELIMINARY VERSION
UNEDITED

CONTENTS

1 BACKGROUND* 1

1.1 National Cyber Security Strategy 1

1.2 Background and Legislative Foundation 2
1.2.1 Origins of the Cyber Security Bill 2
1.2.2 Relaunch of Cyber Security Bill and Key Changes 3

2 DESCRIPTION AND ANALYSIS 4

2.1 Part 1: Amendments to *Telecommunications Act* 4
2.1.1 Canadian Telecommunications Policy Objectives (Clause 1) 4
2.1.2 New Powers (Clause 2) 4
2.1.2.1 Power to Make Orders in Council 5
2.1.2.2 Power to Make Ministerial Orders 6
2.1.2.3 Regulation-Making Power 7
2.1.2.4 Non-disclosure Provision for Orders 7
2.1.2.5 Provision of Information 8
2.1.2.6 Judicial Review of New Powers 10
2.1.3 Compliance of Canadian Radio television and Telecommunications Commission (Clause 3) 10
2.1.4 Inspection and Enforcement (Clauses 4 to 6) 10
2.1.5 New Administrative Monetary Penalties Scheme (Clause 7) 11
2.1.5.1 Violation and Determination of Financial Penalty 11
2.1.5.2 Notices of Violation and Contents of Notice 12
2.1.5.3 Payment, Representations and Compliance Agreements 12
2.1.5.4 Commission of Violation by a Corporation 13
2.1.5.5 End of Proceedings and Limitation Period or Prescription 13
2.1.6 Provisions Common to Administrative Monetary Penalties Schemes and Criminal Offences (Clauses 8 to 10) 14
2.1.6.1 Evidence 14
2.1.6.2 Criminal Offences 14

2.2 Part 2: Critical Cyber Systems Protection Act (Clause 11) 15
2.2.1 Purpose 15
2.2.2 List of Vital Systems and Services and Designated Operators 15
2.2.3 Establishment and Maintenance of Cyber Security Program 16
2.2.4 Mitigation of Supply Chain and Third-Party Risks 17

PRELIMINARY VERSION
UNEDITED

2.2.5 Mandatory Reporting of Cyber Security Incident 18
2.2.6 Secret Cyber Security Directions 19
2.2.6.1 Federal Court Review of Secret Cyber Security Directions 20
2.2.7 Information Disclosure Prohibitions and Permissions 20
2.2.8 Record Keeping 21
2.2.9 Administration and Enforcement of Critical Cyber Systems Protection Act 22
2.2.9.1 Civil Legal Immunity 22
2.2.9.2 Powers of Regulators 22
2.2.9.3 Order for Mandatory Internal Audits 22
2.2.10 Compliance Order Review Requests 23
2.2.11 Regulations 23
2.2.12 Offences and Punishment 24
2.2.12.1 Defences 24
2.2.13 Protection of Solicitor–Client Privilege and Professional Secrecy 25
2.2.14 Annual Report 25

3 COMMENTARY 26

3.1 Regulatory Uncertainty and Implementation Challenges for Designated Operators 26

3.2 Repercussions of New Oversight Powers: Directions and Orders 26

3.3 Concerns About Personal and Confidential Information 28

3.4 Lack of Financial and Technical Support 28

3.5 Repercussions on Contractual Relations and Industry 29

PRELIMINARY VERSION
UNEDITED

LEGISLATIVE SUMMARY OF BILL C-8: AN ACT RESPECTING CYBER SECURITY, AMENDING THE TELECOMMUNICATIONS ACT AND MAKING CONSEQUENTIAL AMENDMENTS TO OTHER ACTS

1 BACKGROUND*

Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts (also referred to as the Cyber Security Act), was introduced in the House of Commons by the Minister of Public Safety and Emergency Preparedness on 18 June 2025.[1] The bill has since been passed by the House of Commons, on 26 March 2026, with amendments.[2] It is currently at second reading in the Senate.

Aiming to strengthen the resilience of Canada's critical infrastructure against growing cyber threats, Bill C-8 establishes a regulatory framework to protect systems and services essential to public safety or national security.[3] Bill C-8 largely mirrors the provisions of Bill C-26, which was introduced in June 2022 during the 44th Parliament.[4] The main differences between the two bills are discussed in the "Background and Legislative Foundation" section of this legislative summary.

This framework has two parts. The first part amends the *Telecommunications Act* to add the security of Canada's telecommunications system as a public policy objective and gives the federal government greater powers to order a telecommunications service provider (TSP) to take measures to counter cyber threats. The second part enacts the Critical Cyber Systems Protection Act (CCSPA), which imposes new cyber security requirements on federally regulated entities operating in sectors that are considered vital to public safety or national security, such as finance, nuclear and electric power, telecommunications and transportation.

1.1 NATIONAL CYBER SECURITY STRATEGY

On 6 February 2025, the Government of Canada announced a new national cyber security strategy called Securing Canada's Digital Future.[5] The strategy highlights the growing speed and complexity of cyber threats, which include a wide range of activities "such as ransomware and cyber-enabled fraud, and uninvited interference in networks and systems" in Canada.[6] According to the government, the resilience of digital infrastructure needs to be strengthened, and citizens, businesses and public institutions must be protected from cyber threats. Bill C-8 is central to the implementation of this strategy, which has three interlocking pillars.

PRELIMINARY VERSION
UNEDITED

The first pillar consists in protecting Canadians and Canadian businesses from cyber threats by collaborating and exchanging information through whole-of-society partnerships. The second pillar is to "make Canada a global cyber security industry leader," in part by supporting innovation, enhancing workforce capacity and targeting key research areas. Lastly, the third pillar is to "detect and disrupt cyber threat actors," including by boosting the federal government's capacity to combat cybercrime and making critical systems more resilient.[7]

In his introductory message for the new strategy, the Minister of Public Safety at the time, the Honourable David J. McGuinty, said that the increase in cyber threats "is creating real impacts for Canadians and is becoming a leading threat to Canada's national security and economy." He stated that the federal government would

> use all available tools to protect Canada's critical infrastructure to better position us to adapt to and combat cyber risks, ensure the security and integrity of Canada's critical systems, and create a mechanism to enforce our 2022 statement on telecommunications security.[8]

Bill C-8 seems to implement this commitment by establishing a legislative framework to protect critical cyber systems by strengthening the federal government's oversight powers and ability to intervene and by imposing specific obligations on operators of vital systems in order to prevent, detect and respond to cyber threats that affect national security.

1.2 BACKGROUND AND LEGISLATIVE FOUNDATION

As mentioned above, Bill C-8 largely reproduces the content of Bill C-26. While the latter completed all stages of the legislative process, a technical error identified by the Senate led to its referral back to the House of Commons, delaying its adoption before it died on the *Order Paper* when Parliament was prorogued in January 2025.[9]

1.2.1 Origins of the Cyber Security Bill

Like Bill C-8, Bill C-26 consisted of two parts. Part 1, which would have amended the *Telecommunications Act*, followed the government's May 2022 announcement that it intends to prohibit the use of Huawei and ZTE products and services in Canada's telecommunications systems, particularly in 5G wireless networks.[10] This decision was consistent with those of Canada's allies – including the United States, the United Kingdom, Australia and Japan – which have also banned Huawei from their 5G networks for national security reasons.[11]

Part 2, which would have created the CCSPA, appeared to be inspired by the Australian model, incorporating several elements of the *Security of Critical Infrastructure Act 2018*[12] and substantive amendments of the *Security Legislation Amendment (Critical Infrastructure) Act 2021*.[13] These 2021 reforms significantly expanded the Australian federal government's powers to enforce cyber security obligations on operators of critical infrastructure and to intervene in case of major cyber incidents. Similarly, the CCSPA would have imposed requirements on designated operators in vital sectors (telecommunications, energy, transportation and finance), such as the creation of cyber security programs, mandatory incident reporting and compliance with government cyber security orders.

This approach was consistent with an international trend toward bolstering the resilience of vital infrastructure against digital threats. For example, the United States' *Cyber Incident Reporting for Critical Infrastructure Act of 2022* requires critical infrastructure operators to report cyber incidents to the Cybersecurity and Infrastructure Security Agency.[14] In the United Kingdom, the reporting requirement is provided by *The Network and Information Systems Regulations 2018*,[15] which is derived from the European Union's 2016 Directive on security of network and information systems (NIS directive).[16] The overarching objective of all these regimes is to achieve an enhanced and common level of security for critical cyber infrastructures while enabling the relevant authorities to better understand and manage cyber risks.

1.2.2 Relaunch of Cyber Security Bill and Key Changes

While Bill C-8 reproduces most of the wording of Bill C-26, it is different in several notable ways. First, it does not include the proposed consequential amendments to the *Canada Evidence Act*, which were intended to give the Federal Court specific jurisdiction over certain matters, including judicial review of orders and regulations made under the *Telecommunications Act* or the CCSPA.[17]

In addition, Bill C-8 makes the judicial review process more transparent by removing the government's ability to make confidential submissions to the court and to refuse to disclose information for national security reasons from section 15.9 of the *Telecommunications Act* (clause 2 of Bill C-26) and section 145 of the CCSPA (clause 12).[18] Moreover, some imprecise wording in Bill C-26 was corrected.[19]

During its consideration by the House of Commons, Bill C-8 was amended in multiple ways, including to limit the scope of the new powers, add a parliamentary review mechanism and clarify the privacy implications of the proposed regime.

PRELIMINARY VERSION
UNEDITED

2 DESCRIPTION AND ANALYSIS

2.1 PART 1: AMENDMENTS TO *TELECOMMUNICATIONS ACT*

Part 1 of the bill contains 10 clauses. Key provisions are discussed in the following sections.

2.1.1 Canadian Telecommunications Policy Objectives (Clause 1)

Clause 1 of the bill makes promoting the security of the Canadian telecommunications system one of the policy objectives of the Canadian Telecommunications Policy, set out in section 7 of the *Telecommunications Act*. The addition allows the Minister of Industry as well as the Canadian Radio-television and Telecommunications Commission (CRTC) to consider this objective when exercising their respective powers under the *Telecommunications Act*. The same consideration is allowed under the *Radiocommunications Act* (the legislation that governs spectrum allocation), which incorporates the *Telecommunications Act*'s objectives by reference.[20]

2.1.2 New Powers (Clause 2)

Clause 2 of the Bill adds sections **15.01** to 15.91 to the *Telecommunications Act* to establish a legislative framework granting the Governor in Council and the Minister of Industry the power to make orders to TSPs. The purpose of the orders must be to secure the Canadian telecommunications system against threats such as interference, manipulation, disruption or degradation, and actions may include specific prohibitions or requirements imposed by order (sections 15.1 and 15.2) or by regulation (section 15.8). Before making an order, the Governor in Council or the minister must also consider certain common factors, the goal being to regulate the exercise of these powers. For example, the scope of an order must be proportional to the gravity of the threat it addresses (new sections 15.1(2) and 15.2(3) of the *Telecommunications Act*). To that end, the Governor in Council or the minister must assess the proposed order's impact on the TSP's operations and financial situation, on the provision of telecommunications services in Canada, including the security and confidentiality of telecommunications, and on the privacy of Canadians. They may also take into account other factors they consider relevant (new sections 15.1(4) and 15.2(6) of the *Telecommunications Act*).

During consideration of Bill C-8, the House of Commons also added section 15.01 to clarify the interpretation of certain key concepts relating to the new powers. This provision limits the concepts of interference, manipulation, disruption and degradation to actions of a technical nature that impede the

operation of a telecommunications system. It explicitly excludes the effects of lawful expression, persuasion or political debate, thus addressing concerns about potential infringement of the freedom of expression guaranteed by the *Canadian Charter of Rights and Freedoms* (the Charter).[21]

Another new section added during House of Commons consideration is section 15.211, which requires the Minister of Industry to give a notice to any person directly affected by an order. If the order does not contain any provision prohibiting its disclosure, the minister must, within seven days after it is made, give a notice containing the order to any person named in it. This requirement helps ensure that affected persons are informed in a timely way of obligations or prohibitions imposed on them.

Sections 15.21(1) to 15.21(3) require the Minister of Industry to table in Parliament a report on the orders made under sections 15.1(1), 15.2(1) and 15.2(2). This report must include the number of orders made and their nature, the providers affected, their degree of compliance and an explanation of their necessity and reasonableness. Moreover, section 15.81 require the Minister to submit to Parliament, within three months after the end of a fiscal year, an annual report respecting any orders referred to in sections 15.1 and 15.2 that were made during that fiscal year. **A summary of the report must also be published on the Department of Industry website within 10 days after it is tabled.** Taken together, these additional measures provide for transparency and accountability by requiring the minister to justify the use of unusual powers before Parliament, allowing for their use and effects to be monitored.

2.1.2.1 Power to Make Orders in Council

New section 15.1 of the *Telecommunications Act* enables the Governor in Council to issue an order prohibiting a TSP from using the products or services of given suppliers, if the Governor in Council is of the opinion that it is necessary to secure the Canadian telecommunications system against any threat **and reasonable in relation to the gravity of the threat**. These measures may include prohibiting a TSP from using the products or services of a particular supplier or ordering it to remove all products provided by that supplier from its networks or facilities (section 15.1(1) of the *Telecommunications Act*).

Section 15.1(7) of the *Telecommunications Act* specifies that the provisions of an order take precedence over any contrary decision, order or authorization.

Section 15.1(8) of the *Telecommunications Act* provides that no one is entitled to any compensation from the federal government for financial losses resulting from the making of an Order in Council.

PRELIMINARY VERSION
UNEDITED

2.1.2.2 Power to Make Ministerial Orders

New section 15.2 of the *Telecommunications Act* gives the Minister of Industry the authority to make orders implementing various measures to secure the Canadian telecommunications system if there are reasonable grounds to believe that they are necessary to secure the Canadian telecommunications system against any threat **and reasonable in relation to the gravity of the threat**. Before exercising this authority, the Minister must consult with the Minister of Public Safety and Emergency Preparedness and any other persons considered important.

Under section 15.2(1), the Minister of Industry may prohibit a TSP from providing services to certain persons or temporarily suspend their provision of services, including to another TSP. **However, an exception was added to section 15.2(1.1) that limits the ability to suspend the provision of services to an individual to cases in which the measure is necessary to secure the Canadian telecommunications system against a specified threat of a technical nature.**

Under new section 15.2(2) of the *Telecommunications Act*, the Minister of Industry may issue an order to

- prohibit a TSP from using any specified product or service in its networks or facilities;
- direct a TSP to remove a specified product from all or part of its networks or facilities;
- impose conditions on a TSP's use of any product or service, or on the TSP's provision of service to a specified person;
- prohibit a TSP from upgrading any specified product or service;
- subject a TSP's networks or facilities, as well as its procurement plans for those networks or facilities, to specified review processes;
- require a TSP to develop a security plan in relation to its services, networks or facilities;
- require a TSP to conduct an assessment to identify any vulnerabilities in its services, networks, facilities or security plan; and
- require a TSP to take steps to mitigate any vulnerabilities identified in its assessment.

During its consideration of Bill C-8, the House of Commons tightened the rules governing these powers by specifying that the minister cannot order the decoding of an encrypted private communication (section 15.2(2.1)) or the

interception of a private communication or a radio-based telephone communication, as defined in section 183 of the *Criminal Code*[22] (section 15.2(4)).[23]

New section 15.2(9) of the *Telecommunications Act* specifies that, in case of a conflict, an order made under the *Telecommunications Act* prevails over any other measure, including a decision of the CRTC and ministerial orders or authorizations under the *Telecommunications Act* or the *Radiocommunication Act*.

As with an order in council, no one is entitled to any compensation from the federal government for any financial losses resulting from a ministerial order, pursuant to new section 15.2(10) of the *Telecommunications Act*.

2.1.2.3 Regulation-Making Power

Under new section 15.8(1) of the *Telecommunications Act*, the Governor in Council may make regulations covering anything that may be included in one of the ministerial orders made under section 15.2 of that Act. Regulations can also be used to designate persons or entities that may collect and disclose information covered by the relevant provisions of the *Telecommunications Act*.

The regulations made under new section 15.8(1) take precedence over any decision, order or authorization by the CRTC or the minister, including those issued under the *Radiocommunication Act* (section 15.8(2)).

2.1.2.4 Non-disclosure Provision for Orders

Although the bill requires the Governor in Council or the Minister of Industry to publish orders in council and ministerial orders in the *Canada Gazette* within 90 days of their adoption (new sections 15.1(6) and 15.2(8) of the *Telecommunications Act*), it also allows them to keep these orders secret by including non-disclosure provisions prohibiting any person concerned from revealing the existence or content, even in part, of the order in question (sections 15.1(3) and 15.2(5)).

New sections 15.3(1) to 15.3(4) of the *Telecommunications Act* set out the conditions of enforcement for orders made under sections 15.1 and 15.2. They clarify that no person can be penalized for contravening an order unless it is proved that they were notified of it, which can be done with a certificate signed by the minister.

The House of Commons adopted an amendment to further constrain the exercise of these powers. Sections 15.1(3.1) and 15.2(5.1) provide that, before prohibiting disclosure, the Minister of Industry must consider a number of factors, including the risk that the disclosure could compromise the objective of

the order, the necessity and scope of the prohibition relative to the threat, the effect of non-disclosure on the principles of government transparency and accountability, and any representations made by the affected TSPs.

Furthermore, pursuant to section 15.22, the minister must, within 90 days, notify the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency of any measure that includes a non-disclosure provision.

These provisions play a key role in balancing national security and fundamental rights. They enable the government to make certain measures confidential (sections 15.1(3) and 15.2(5)) while providing that no penalty can be imposed without proof that the person in question had been informed of them (sections 15.3(1) to 15.3(4)).

2.1.2.5 Provision of Information

Sections 15.4 to 15.71 of the *Telecommunications Act* govern the collection, designation, exchange and disclosure of information that is relevant to the making or amending of regulatory measures (orders or regulations) relating to telecommunications security.

New section 15.4 allows the Minister of Industry to order any person to provide information that they believe is reasonable to provide relative to the gravity of the threat and necessary to the making, amending or revoking of an order under section 15.1 or 15.2, or a regulation under section 15.8(1)(a) of the *Telecommunications Act*, or to verifying compliance or preventing non-compliance with such an order or regulation.

New section 15.5(1) governs the confidentiality of the information provided under section 15.4 by enabling the person who provides it to designate some of it as confidential, including financial, commercial, scientific or technical information and personal and de-identified information. **To better protect privacy, section 15.5(2.1), which was added during consideration of Bill C-8 at the House of Commons, stipulates that personal information and de-identified information that is not expressly designated as confidential is deemed to be so designated.**

In addition, amendments made to section 15.5(2) while Bill C-26 was being considered added definitions to clarify the concepts of "personal information" and "de-identify." The goal was to improve understanding and the application of the privacy protections. **Providing information designated as or deemed to be confidential is prohibited, subject to certain exceptions set out in sections 15.5(3) to 15.5(5), such as if the disclosure is required by law or considered necessary by**

the minister to secure the Canadian telecommunications system against a serious threat.

Sections 15.6 to 15.71 of the *Telecommunications Act* specify the terms and conditions for the exchange of information between federal departments and agencies with security mandates while strengthening the guarantees protecting personal and confidential information. While the *Telecommunications Act* currently has provisions allowing information sharing between the CRTC and Innovation, Science and Economic Development Canada, new section 15.6 broadens this framework to include ministers of other departments and national security entities.

In this regard, new section 15.6(1.1) more strictly regulates the collection and disclosure of the personal information and de-identified information referred to in section 15.5(1)(d) by requiring that its scope and substance be reasonable relative to the threat in question.

Section 15.7 authorizes the Minister of Industry to disclose, under an agreement, memorandum of understanding or arrangement in writing with provincial or international partners, information collected under the *Telecommunications Act*, except information designated as confidential. **This disclosure is conditional on the minister believing that the information may be relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state and the agreement, memorandum of understanding or arrangement providing additional guarantees, including a requirement to dispose of the information once it is no longer necessary for the purpose for which it was disclosed.**

Moreover, section 15.701, which was added during House of Commons consideration of Bill C-8, imposes an explicit duty to dispose of personal information and de-identified information collected or obtained under such an agreement, memorandum of understanding or arrangement if it is no longer necessary for purposes relating to the powers granted by sections 15.1, 15.2 or 15.8 or in accordance with the applicable requirements of the *Privacy Act.*[24]

Finally, section 15.71 confirms that these provisions must be consistent with the *Privacy Act*, **while section 15.72 adds a specific prohibition to protect the identity of individuals who voluntarily provide information to the minister and ask to remain anonymous**. Together, these provisions strike a balance between national security and privacy by providing a legal framework for managing confidential information.

PRELIMINARY VERSION
UNEDITED

2.1.2.6 Judicial Review of New Powers

Sections 15.9 and 15.91 of the *Telecommunications Act* establish the rules for judicial review of and appeals respecting orders and regulations made under sections 15.1, 15.2 and 15.8(1)(a) of the *Telecommunications Act*.

Section 15.9 provides that a judge conducting such a review must exclude from their decision any evidence they consider irrelevant and any evidence withdrawn by the Minister of Industry and must keep it confidential. The goal is to protect sensitive information while allowing for judicial scrutiny. Section 15.91 extends these same rules to appeals of these decisions, ensuring information is protected throughout the judicial process.

2.1.3 Compliance of Canadian Radio television and Telecommunications Commission (Clause 3)

Clause 3 amends section 47 of the *Telecommunications Act* to require the CRTC to consider any orders of the Governor in Council or the Minister of Industry when exercising its powers and duties under that Act.

2.1.4 Inspection and Enforcement (Clauses 4 to 6)

Clauses 4 to 6 amend sections 71 and 72 of the *Telecommunications Act* to strengthen the powers of the Minister of Industry with respect to inspecting and verifying compliance with the new obligations.

Clause 4 amends section 71 of the *Telecommunications Act* to integrate the new powers to make orders (sections 15.1 and 15.2) and regulations (section 15.8(1)(a)) into the existing inspection and enforcement regime. Accordingly, the new wording of section 71 allows the Minister of Industry to designate inspectors to verify compliance or to prevent non-compliance with any orders or regulations issued using the new powers provided for in this bill.

Lastly, clauses 5 and 6 amend sections 72(3) and 72.001 of the *Telecommunications Act* to specify the legal consequences of non-compliance with the new obligations. Under section 72(1) of the *Telecommunications Act*, a person who has incurred a loss or damage because as a result of a breach of the provisions of the *Telecommunications Act* (or any orders or regulations made under that Act) may sue the offender for an amount equal to the loss or damage. Section 72(3) prevents civil actions against businesses complying with cyber security orders and regulations, protecting them from unwarranted contract-related proceedings.

PRELIMINARY VERSION
UNEDITED

As for section 72.001, it provides that the new order-making powers under the *Telecommunications Act* are not subject to that Act's general administrative monetary penalties scheme. Instead, the bill establishes a separate administrative monetary penalties scheme for violations of these new powers. These provisions reflect an intent to ensure compliance while protecting service providers from the legal risks of implementing national security measures.

2.1.5 New Administrative Monetary Penalties Scheme (Clause 7)

Clause 7 of Bill C-8 creates a new administrative monetary penalties scheme specifically for the security of the Canadian telecommunications system by adding sections 72.131 to 72.1393 to the *Telecommunications Act*.

2.1.5.1 Violation and Determination of Financial Penalty

New section 72.131 of the *Telecommunications Act* provides that a person who contravenes to orders or regulation made under section 15.1, 15.2 or 15.8(1)(a) of that Act commits a violation liable to a financial penalty. For instance, failing to comply with an order requiring the provision of data on the pricing practices of a provider or disclosing confidential information to a third party without authorization could constitute such a violation.

Individuals may incur a penalty of up to $25,000 for a first violation and up to $50,000 for a subsequent contravention. In other cases, such as for businesses, the financial penalty may be up to $10 million for a first violation and up to $15 million for a subsequent contravention (new section 72.131 of the *Telecommunications Act*). These amounts reflect the seriousness of cyber security issues and the legislative intent to deter any negligence or non-compliance in vital sectors.

Section 72.132 of the *Telecommunications Act* adds the concept of a continuing violation and specifies that a violation that persists constitutes a separate violation for each additional day. This provision is designed to discourage delays in compliance by significantly increasing the administrative monetary penalties.

In addition, new section 72.133(1) of the *Telecommunications Act* lists the criteria that the Minister of Industry must consider when determining the amount of the penalty, such as the nature and scope of the violation, the history of compliance of the person who committed the violation and the person's ability to pay the penalty. According to new section 72.133(2), while the bill establishes a system of administrative monetary penalties, the purpose of the penalty is not to punish but to promote compliance with orders and regulations.

PRELIMINARY VERSION
UNEDITED

2.1.5.2 Notices of Violation and Contents of Notice

New sections 72.134 and 72.135 of the *Telecommunications Act* clarify the roles of the Minister of Industry and the persons designated to issue notices of violation in the implementation of the new penalty scheme while ensuring administrative efficiency and upholding the procedural rights of the persons affected.[25]

For example, under new section 72.134, the minister may designate the persons authorized to issue notices of violation or enter into compliance agreements. The minister can also establish a short-form description for use in such notices.

New section 72.135 establishes the procedure for notices of violation. It provides that a designated person can issue a notice of violation if they believe, on reasonable grounds, that a violation has been committed. This document must be served on the person concerned and must name the person, state the violation, include the amount of the penalty and list the options available to the person: either pay the penalty or make representations to the minister within 30 days (or a longer period, at the minister's discretion). The provision also stipulates that, if the person fails to act in accordance with the notice, they will be deemed to have committed the violation.

For as long as no representation has been made, the designated person may correct or cancel the notice, which enables any administrative error to be corrected quickly without formal proceedings.

2.1.5.3 Payment, Representations and Compliance Agreements

New sections 72.136 and 72.137 of the *Telecommunications Act* establish the administrative monetary penalty process by delineating the roles of the Minister, designated officials, and persons served with a notice of violation, including the consequences of payment, failure to respond, ministerial determinations, and the operation of compliance agreements.

New section 72.136 clarifies the consequences of payment or the making of representations. In every case, payment of the penalty constitutes an admission of liability and terminates the proceedings.

However, if a person served with a notice of violation makes representations to the minister, the minister must decide, on a balance of probabilities, after considering the representations, whether the person committed the violation. The minister may then impose, reduce or cancel the penalty.

Failure to pay or submit representations in the time allotted also constitutes an admission of liability and allows the Minister to impose the penalty indicated in the

statement of offence. A copy of this decision is then served on the concerned person, ensuring transparency and formal end to the process.

New section 72.137 allows a designated person to enter into a compliance agreement with the person believed to have committed the violation. The agreement is subject to any terms found appropriate and may provide for a reduction or elimination of the penalty.

Once a compliance agreement has been entered into, the person is deemed to have committed the violation, and they may not make representations. If the compliance agreement is complied with, notice of this is given, which ends the proceedings.

In the event of non-compliance with the compliance agreement, a notice of default is issued requiring the person to pay the initial penalty, less any amount already paid. Payment consistent with this notice also ends the proceedings. This mechanism provides an alternative to formal challenges while ensuring the administrative process is efficient and definitive.

2.1.5.4 Commission of Violation by a Corporation

Under new section 72.138 of the *Telecommunications Act*, when a corporation is believed to have committed a violation, its officers, directors, agents or mandataries are liable for the violation if they directed, authorized, assented to, acquiesced in or participated in the commission of the violation, whether or not the corporation is proceeded against.

2.1.5.5 End of Proceedings and Limitation Period or Prescription

New sections 72.139 to 72.1393 of the *Telecommunications Act* complete the administrative monetary penalties scheme with a series of provisions regarding recovery, the limitation period or prescription, transparency and regulations.

Section 72.139 provides that a penalty and any interest due in respect of it are a debt due to His Majesty that is recoverable in Federal Court or any other court of competent jurisdiction. A proceeding to recover that debt may not be commenced more than five years after the debt becomes payable, and any penalty is payable to the Receiver General. In addition, the Minister of Industry may issue a certificate for the unpaid amount that, once registered in Federal Court, has the same effect as a judgment of that court. This enables the government to efficiently recover all amounts due while ensuring a sound legal foundation for carrying out its decisions.

Section 72.1392 authorizes the minister to publish the name of a person who commits a violation, the nature of the violation and any compliance agreement entered into

PRELIMINARY VERSION
UNEDITED

and the penalty amount. This provision strengthens transparency and deters non-compliant conduct.

Lastly, section 72.1393 enables the Governor in Council to make regulations to exempt certain provisions from the application of penalties (section 72.131 of the *Telecommunications Act*), establish other factors to be considered in determining penalty amounts (section 72.133(1)(e) of the *Telecommunications Act*) and govern the terms and conditions of compliance agreements provided by section 72.137. These regulatory powers allow for adapting the scheme to operational realities and enable flexible and efficient implementation.

2.1.6 Provisions Common to Administrative Monetary Penalties Schemes and Criminal Offences (Clauses 8 to 10)

The *Telecommunications Act* relies on both an administrative monetary penalties scheme (section 72.14) and a criminal offence scheme (section 73). Clauses 8 to 10 of Bill C-8 make changes to sections 72.14 and 73 of the *Telecommunications Act* to include rules of evidence, expand criminal liability and strengthen the judicial tools the government can use to ensure compliance with the new cyber security obligations.

2.1.6.1 Evidence

Clause 9 amends section 72.14 of the *Telecommunications Act* to specify that, in a proceeding in respect of a violation, a notice or a copy of the decision purporting to be served in the application of this provision is admissible as evidence without necessity to prove the authenticity of the signature or the official capacity of the signatory.

2.1.6.2 Criminal Offences

The amendments to section 73 of the *Telecommunications Act* add to the criminal penalties scheme violations of orders and regulations made under sections 15.1, 15.2 and 15.8(1)(a) of that Act.

New section 73(3.1) provides that an individual found to have committed such an offence is liable to a fine and to imprisonment for up to two years less a day, while a corporation is liable to a fine only.

New sections 73(3.2) to 73(3.5) extend criminal liability to officers, directors, agents or mandataries who participated in the commission of the offence and allow a person to be held liable for the actions of their employees, agents or mandataries. It is a defence for a person in a proceeding in relation to a violation, under new section 73(3.4) of the *Telecommunications Act*, to establish that the person exercised all due diligence to prevent the commission of the offence.

PRELIMINARY VERSION
UNEDITED

Finally, section 73(7) is amended to enable the court of competent jurisdiction to issue an injunction if it is satisfied that a violation of a cyber security provision is being committed or is imminent. This injunction may require any person to cease or refrain from any activity related to the violation, giving the Minister of Industry a judicial tool to prevent breaches of the security of the Canadian telecommunications system.

2.2 PART 2: CRITICAL CYBER SYSTEMS PROTECTION ACT (CLAUSE 11)

Clause 11 of the bill enacts the CCSPA. Key provisions of the CCSPA are discussed in the following sections.

2.2.1 Purpose

The stated purpose of the CCSPA is to protect critical cyber systems in order to ensure the continuity and security of vital systems and services in Canada (section 5 of the CCSPA). These systems and services are considered vital to national security, public safety and the proper operation of infrastructure under federal jurisdiction.

More specifically, the CCSPA aims to enable authorities and operators to better identify and manage cyber security risks, including those associated with supply chains and the use of third-party products and services (section 5(a)). It also seeks to prevent any compromise of critical cyber systems (section 5(b)), to quickly detect any cyber security incidents that are affecting or that could affect those systems (section 5(c)) and to minimize the impacts of such incidents should one occur (section 5(d)).

In sum, the CCSPA creates a legislative framework to prevent, detect and respond to cyber threats that could compromise Canada’s critical infrastructure.

2.2.2 List of Vital Systems and Services and Designated Operators

Sections 6 and 7 of the CCSPA respectively empower the Governor in Council to order the addition or modification of federally regulated “vital services and vital systems” in Schedule 1 of the CCSPA and to add or modify designated operators and regulators of these vital services and systems in Schedule 2 of the CCSPA.

Schedule 1 currently identifies six vital services and systems: telecommunications services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems that are within the legislative authority of Parliament, banking systems, and clearing and settlement systems.

PRELIMINARY VERSION
UNEDITED

2.2.3 Establishment and Maintenance of Cyber Security Program

Section 9 of the CCSPA requires designated operators in vital sectors to establish a cyber security program within 90 days after an order is published under section 7 and they become a member of a class of operators listed in Schedule 2.

Section 9(1) of the CCSPA specifies the expected outcomes of this cyber security program. They include:

- identifying and managing any cyber risks to the organization, including supply chain risks and risks posed by third-party products and services;
- protecting critical cyber systems from being compromised;
- detecting any cyber security incidents that could affect or that are affecting critical cyber systems; and
- limiting damage in the event of a cyber security incident affecting critical cyber systems.

A critical cyber system is defined under section 2 of the CCSPA as "a cyber system that, if its confidentiality, integrity or availability were compromised, could affect the continuity or security of a vital service or vital system." A "cyber security incident" is defined as "an incident, including an act, omission or circumstance, that interferes or may interfere with" the continuity or security of a vital service or system, or the confidentiality, integrity or availability of a critical cyber system.

Section 9(1)(e) requires designated operators to "do anything that is prescribed by the regulations," which suggests federal government directives on cyber security programs for vital services and systems will be issued on an ongoing basis.

Section 9(2) of the CCSPA requires designated operators to immediately notify in writing the "appropriate regulator"[26] that they have established a cyber security program.

Under section 10 of the CCSPA, a designated operator has 90 days following its designation under Schedule 2 to make its cyber security program available to the regulator. Under Schedule 2, each designated operator belongs to a class of operators and each class of operators has a specified regulator to whom they must report.

Section 11 of the CCSPA allows for an extension of the 90-day deadline, upon a written request to the appropriate regulator, to allow the designated operator to comply with the requirements of section 9(1) or section 10.

PRELIMINARY VERSION
UNEDITED

Section 12 of the CCSPA requires designated operators to not only implement their cyber security programs but also maintain them over time. The CCSPA sets out two mechanisms to ensure cyber security programs remain up to date: regulations and program reviews.

Section 13 of the CCSPA stipulates that designated operators must conduct a periodic review of their cyber security program at least once a year, either on the date prescribed by regulation or on the anniversary of its establishment. This review must be completed within a 60-day period, unless otherwise specified, and may entail changes to the program. The operator must inform the regulator of whether they have made any changes to their program within 30 days after completing that review.

Finally, section 14 of the CCSPA requires notification of any material changes in ownership, supply chains or any other circumstance prescribed by regulation. Further notification must be provided within 90 days to indicate whether the program has been changed, and this deadline can be extended.

2.2.4 Mitigation of Supply Chain and Third-Party Risks

Section 15 of the CCSPA requires designated operators to mitigate risks related to their supply chain or use of third-party cyber security products and services as soon as these risks are identified. Designated operators must take reasonable steps, including those that may be prescribed through regulation, to mitigate these risks "as soon as" they are discovered.

The House of Commons added section 15.1 of the CCSPA to grant the Communications Security Establishment (CSE) the power to develop, in consultation with industry stakeholders, specific guidelines on mitigating the risks associated with supply chains and the use of third-party products and services. These guidelines may take into account internationally recognized frameworks, including those developed by the International Organization for Standardization respecting cyber security in supplier relationships. While these guidelines are not regulations, they would orient the application of the mitigation requirements set out in section 15 of the CCSPA, including by promoting the adoption of practices consistent with recognized cyber security frameworks.

The regulator is authorized, under section 16 of the CCSPA, to disclose to CSE any information, including confidential information concerning a designated operator's cyber security program and the risk mitigation measures provided for in section 15, to obtain "advice, guidance, and services."

Section 2 of the CCSPA defines "confidential information" as information whose disclosure could compromise the security or competitiveness of a designated operator. This definition is based on three principles: first, information on the "vulnerability of [a] critical cyber system" or the protection methods used is considered confidential if it "is consistently treated as confidential by the designated operator." Second, information whose disclosure "could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a designated operator" is considered confidential. Third, information is considered confidential if its disclosure "could reasonably be expected to interfere with contractual or other negotiations of a designated operator."

2.2.5 Mandatory Reporting of Cyber Security Incident

Sections 17 to 19 of the CCSPA establish clear cyber security incident reporting requirements for designated operators.

Section 17 directs designated operators to report to CSE any cyber security incident involving their critical cyber systems within the prescribed period, which cannot exceed 72 hours. This period was extended during consideration of Bill C-26 to enable CSE to carry out its cyber security oversight, analysis and intervention duties while allowing designated operators to respond effectively to a serious incident.[27]

Under section 18(b) of the Communications Security Establishment Act (CSE Act),[28] CSE is mandated to carry out cyber defence operations to help protect "electronic information and information infrastructures designated … as being of importance to the Government of Canada."

After an incident is reported to CSE, section 18 requires designated operators to "immediately" notify the appropriate regulator and provide it with a copy of the incident report. This dual notification ensures the technical authority (the CSE) and the relevant sectoral regulatory authorities coordinate their actions, which strengthens the government's response capacity.

New section 18.1 of the CCSPA clarifies that the reporting requirements set out in sections 17 and 18 do not affect the provisions of the *Personal Information Protection and Electronic Documents Act*.[29] This clarification confirms that the mandatory cyber security incident reporting regime must be implemented in a manner consistent with the general rules governing the collection, use and disclosure of personal information.

Finally, section 19 of the CCSPA enables the appropriate regulator to ask CSE to provide a copy or a portion of an incident report for the purpose of verifying

legislative and regulatory compliance with the CCSPA. This provision facilitates information sharing between government entities while ensuring regulatory oversight of designated operators.

Together, these provisions establish a strong framework for reporting, transparency and inter-institutional cooperation, which is essential to protecting critical cyber systems from growing digital threats, all while ensuring compliance with the applicable privacy requirements.

2.2.6 Secret Cyber Security Directions

Sections 20 through 23 of the CCSPA empower the Governor in Council to issue, by order, secret "cyber security directions" to designated operators, provided that there are reasonable grounds to believe that such measures are necessary to protect a critical cyber system. Under section 20 of the CCSPA, these directions can be amended or revoked and must reflect a number of factors, including their operational impacts, public safety, **the privacy of Canadians,** operators' finances and the delivery of vital services. Designated operators who are subject to a direction are required to comply with it.

The Minister of Public Safety and Emergency Preparedness must, within 90 days of making a directive, notify the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency of the making of the order. In addition, these directives cannot authorize the interception of private communications within the meaning of the *Criminal Code*. Section 21 governs the contents of the directions, which must set out to whom they apply, the measures to be taken, any associated conditions and the time allowed for them.

The secrecy and speed of these directions are enabled by section 22(1) of the CCSPA, which exempts cyber security directions from sections 3, 5 and 11 of the *Statutory Instruments Act* (SIA).[30] Section 3 of the SIA requires that proposed regulations be examined in consultation with the Deputy Minister of Justice for, among other things, compliance with the Charter. Section 5 of the SIA requires that all regulations be transmitted in both official languages to the Clerk of the Privy Council for registration, and section 11 requires that all regulations be published in the *Canada Gazette* within 23 days of registration.

However, section 22 of the CCSPA provides that an operator cannot be found to have contravened a direction unless it is proved that it had been notified of it or that reasonable steps had been taken to notify it.

Section 23 of the CCSPA authorizes the exchange of information, including confidential information, between a number of federal departments and agencies –

PRELIMINARY VERSION
UNEDITED

including CSE, the Canadian Security Intelligence Service, the Department of National Defence and the Department of Foreign Affairs – to the extent necessary for the making, amending or revoking of a direction. All these entities must treat this information as confidential.

Lastly, under sections 24 and 25 of the CCSPA, designated operators that are subject to a cyber security direction are prohibited from disclosing or allowing others to disclose the contents of the direction or even the fact that the direction was issued, unless the disclosure is necessary to comply with the direction.

2.2.6.1 Federal Court Review of Secret Cyber Security Directions

Sections 145 and 146 of the CCSPA set out the specific rules for judicial review of cyber security directions issued under section 20 of the CCSPA.

Section 145 of the CCSPA provides for judicial review of cyber security directions by a Federal Court judge. Section 145(1) provides that, in judicial review proceedings regarding a cyber security direction, the judge cannot base their decision on evidence or information that the judge determines to be irrelevant or that the Minister withdraws. The judge must inform the minister and ensure the confidentiality of all evidence and other information withdrawn from the proceedings. This rule is intended to protect classified or sensitive information while enabling the court to rule on the legality of the direction.

Section 146 of the CCSPA extends these rules to appeals of decisions made in such a judicial review, ensuring procedural consistency and ongoing protection of confidential information throughout the judicial process.

2.2.7 Information Disclosure Prohibitions and Permissions

Sections 26 to 29 of the CCSPA address the disclosure and use of information collected under the CCSPA. While the CCSPA prohibits knowingly disclosing or allowing the disclosure of confidential information, it also creates a list of exceptions, including in section 26(1)(f) for disclosure under the *Security of Canada Information Disclosure Act*,[31] which allows the disclosure of information among 17 federal departments and agencies in order to protect Canada from "activities that undermine the security of Canada."

Section 26(1)(b) of the CCSPA creates an exception to the prohibition against disclosure for "publicly available information." At present, section 2 of the CSE Act provides the most expansive definition of publicly available information in Canadian law, defining it as "information that has been published or broadcast for public

PRELIMINARY VERSION
UNEDITED

consumption, is accessible to the public on the global information infrastructure … or is available to the public on request, by subscription or by purchase."[32]

New section 26.1 was added to the CCSPA during House of Commons consideration. It specifies that the provisions of the CCSPA do not affect the requirements of the *Privacy Act*. For the purposes of the CCSPA, "personal information" has the same meaning as it does under section 3 of the *Privacy Act*, as provided by the definition in section 2 of the CCSPA. Section 26.1 of the CCSPA therefore confirms that, despite the exceptions set out in section 26, the collection, use and disclosure of personal information continues to be governed by the general legislative framework applicable to the federal public sector.

Section 27 of the CCSPA permits the Minister of Public Safety, responsible ministers and regulators to enter into a written information-sharing agreements or arrangements with provincial governments, foreign states or international organizations established by the governments of foreign states. Exchanges of information under these agreements or arrangements must relate to the protection of critical cyber systems, and with the exception provided for provincial governments under section 27(2), cannot include confidential information.

Section 29 of the CCSPA grants the appropriate regulator the power to require any person, partnership or unincorporated organization to provide it with any information it requires to verify compliance or prevent non-compliance with the provisions of the CCSPA or its regulations. The information must be provided within the time and in the manner stipulated in the request, which allows for some administrative flexibility while ensuring the verification process is efficient.

Section 29.1 is a new addition that introduces an explicit duty to dispose of personal information collected or obtained under the CCSPA if it is no longer necessary for the purposes for which it was collected or for verifying compliance or preventing non-compliance with the CCSPA, consistent with the applicable requirements of the *Privacy Act*. Finally, section 29.2 provides that the CCSPA does not affect the provisions of the CSE Act as regards the protection of personal information, which confirms the coexistence and complementary nature of the applicable protection frameworks.

2.2.8 Record Keeping

Section 30 of the CCSPA requires designated operators to maintain records on the key features of their respective cyber security programs, including steps taken to mitigate supply chain or third-party risks, all reported cyber security incidents, measures taken to implement cyber security directions and any other items prescribed by the regulations.

PRELIMINARY VERSION
UNEDITED

Section 30(2) requires these records to be kept within Canada, at a place and in a manner prescribed by regulation. In the absence of precision under regulations, records are to be maintained at the designated operator's place of business.

2.2.9 Administration and Enforcement of Critical Cyber Systems Protection Act

To facilitate the implementation of and compliance with the CCSPA, the legislation includes limitations on the legal liability of those who implement it and a framework governing the powers of the six regulatory agencies responsible for overseeing the operation of critical systems and services.

2.2.9.1 Civil Legal Immunity

Section 31 of the CCSPA provides legal immunity to persons who exercise powers or perform duties or functions under that Act and those who accompany them. The goal of this provision is to protect government officials and authorized persons from all civil liability when they act in good faith in carrying out their responsibilities.

2.2.9.2 Powers of Regulators

Sections 32 to 85 of the CCSPA set out the powers of each of the six regulators assigned to oversee the operation of vital services and systems.

For the purpose of verifying compliance or preventing non-compliance with the CCSPA and its regulations, each of these six regulators is permitted to enter any place – other than a dwelling-house – without consent or a warrant (sections 32, 41, 50, 59, 68 and 78). The CCSPA requires the regulator to obtain a warrant from a justice of the peace through an *ex parte* application to enter a dwelling-house (sections 33, 42, 51, 60, 69 and 79).

Upon entry to a place, a regulator may examine, use or cause to be used any cyber system to obtain information from it, among other things. The regulator may then prepare or cause to be prepared a document capturing this information. The regulator also has authority to examine and copy any record, report, data or any other document in the place, using copying equipment found in the place, if required. Lastly, the regulator is authorized to remove any document, record or cyber system – in part or in whole – from the place in order to examine or copy it.

2.2.9.3 Order for Mandatory Internal Audits

Under sections 34, 43, 52, 61, 70 and 80 of the CCSPA and subject to the regulations, a regulatory body may order in writing a designated operator to conduct an internal audit within a prescribed period to determine its compliance with the CEPA and its

PRELIMINARY VERSION
UNEDITED

regulations. As these orders are exempt from the SIA, they are not published in the *Canada Gazette* and are therefore not public.

Sections 35, 44, 53, 62, 71 and 81 require the designated operator to report the findings of its audit to the regulator. Where the designated operator has determined that there is non-compliance, the designated operator's report to the regulator must identify the nature of the non-compliance and describe the measures the designated operator will take to comply.

If a regulator has reasonable grounds to believe that a designated operator is or will likely be in contravention of the CCSPA or any of its regulations, sections 36, 45, 54, 63, 73 and 82 of the CCSPA empower the regulator to order the designated operator to stop doing, or cause to be stopped, whatever is or is likely in contravention within a specified period. Likewise, the regulator may order the designated operator to take measures to mitigate the effects of non-compliance. Again, under sections 36(3), 45(3), 54(3), 63(3), 73(4) and 82(3), these compliance orders are not made public.

Sections 37, 46, 55, 64, 74 and 83 of the CCSPA state explicitly that a designated operator subject to such an order must comply with it and immediately notify the appropriate regulator when it has complied.

2.2.10 Compliance Order Review Requests

A designated operator subject to a compliance order may submit a written request to the regulator to review the order (sections 38, 47, 56, 65, 84 and 75(2) to 75(4) of the CCSPA). The review request must be submitted in the time and manner set out in the compliance order, state the grounds for the review and provide supporting evidence for the review. However, unless the regulator decides otherwise, the compliance order stands during the review.

Once the regulator has completed a compliance order review, sections 39, 48, 57, 66, 76 and 85 of the CCSPA require the regulator to confirm, amend, revoke or cancel the order and provide notice of this decision and the reasons for it to the designated operator. Alternatively, if the regulator has not made a decision within 90 days after receiving a review request or after any other period that has been mutually agreed to by the regulator and designated operator, the regulator is deemed to have confirmed the original compliance order.

2.2.11 Regulations

Section 135 of the CCSPA grants the Governor in Council the power to make regulations to carry out the CCSPA.

PRELIMINARY VERSION
UNEDITED

More specifically, section 135(1) lists a series of areas in which regulations can be made. They include cyber security programs, internal audits, the way cyber security incidents are reported (including those referred to in section 17 of the CCSPA), the period for notifications of changes (section 14), the management of records (section 30) and the classification of violations (minor, serious or very serious) and the applicable maximum penalties. The Governor in Council can also define any undefined words or expressions in the CCSPA and prescribe anything that is to be prescribed under it.

Section 135(2) adds that, in making these regulations, the Governor in Council may seek to ensure consistency with existing regulatory regimes, including those of provincial agencies. This provision reflects a desire for intergovernmental harmonization, which is essential in a field such as cyber security, where infrastructure and responsibility may be shared by different levels of government.

2.2.12 Offences and Punishment

Sections 136 to 146 of the CCSPA establish a complete scheme of offences, criminal penalties and judicial procedures to ensure compliance with the requirements of that Act.

Section 136 provides that any person who contravenes a series of specific requirements – such as providing a cyber security program (section 10 of the CCSPA), reporting incidents (section 17) or keeping records (section 30) – is guilty of a summary conviction offence.

Section 137 goes further by providing that some offences, such as non-compliance with a cyber security direction (section 20(4) of the CCSPA) and the prohibited disclosure of a direction (section 24), may be prosecuted summarily or by indictment, with penalties of up to five years of imprisonment for individuals and unlimited fines at the court's discretion for corporations.

Section 138 specifies that directors or officers who participated in the commission of an offence are considered parties to the offence and may be prosecuted even if the designated operator is not. Section 139 introduces the concept of a continuing offence, which provides for a separate offence for each day on which the violation continues, which can increase penalties substantially. Finally, section 140 establishes a limitation period or prescription of three years for launching a prosecution.

2.2.12.1 Defences

Defences are also detailed. Section 141 of the CCSPA allows an accused to be absolved if they can prove that they exercised all due diligence to prevent the commission of the offence. Section 142 of the CCSPA eases the burden of proof by

PRELIMINARY VERSION
UNEDITED

allowing an offence to be proved by an employee or agent or mandatary's commission of the offence, even if that person is not identified or prosecuted.

Lastly, sections 143 and 144 of the CCSPA facilitate the production of evidence by recognizing the evidentiary value of certified documents and entries in records. Sections 145 and 146 of the CCSPA govern the rules for judicial review of cyber security directions, in part by ensuring the confidentiality of sensitive information provided to the court.

2.2.13 Protection of Solicitor–Client Privilege and Professional Secrecy

Lastly, new section 148 of the CCSPA provides that the CCSPA is not to be construed as affecting solicitor-client privilege or, in Quebec, the professional secrecy of advocates and notaries. This provision confirms that, despite the scope of the investigatory, information disclosure and judicial review powers under the CCSPA, the recognized protections for solicitor-client privilege and professional secrecy remain fully effective. Consequently, it preserves a fundamental principle of the administration of justice, including during criminal, regulatory and judicial proceedings under the CCSPA.

2.2.14 Annual Report

Section 147 of the CCSPA directs the Minister of Public Safety to prepare a report on the administration of the CCSPA within three months after the end of each fiscal year and to table this report in the Senate and the House of Commons within the first 15 sitting days after the report's completion.

Section 147(2) specifies that the report must contain detailed information on the orders made under section 20(1) of the CCSPA, including the number of directions made and revoked, the number of designated operators affected and descriptions of their level of compliance – full or partial – with the directions they received. The report must also explain the necessity, proportionality and utility of the directions.

Finally, section 147(3) requires the report to include data on the number of directions issued over the previous fiscal year, the number of operators affected and any other information the minister considers relevant, as long as it does not reveal the identity of the operators or persons involved.

PRELIMINARY VERSION
UNEDITED

3 COMMENTARY

Since it was introduced, Bill C-8 has sparked many reactions from stakeholders. This part provides an overview of how stakeholders have analyzed the bill, including the viewpoints of academics, legal professionals, civil rights advocates and experts in cyber security and public law.

A Charter statement for Bill C-8 was published in September 2025.[33] This statement provided legal information on some of the concerns stakeholders have raised, particularly those relating to the scope of the powers conferred on the executive, the protection of personal information and the potential impacts on the rights and freedoms guaranteed by the Charter.

3.1 REGULATORY UNCERTAINTY AND IMPLEMENTATION CHALLENGES FOR DESIGNATED OPERATORS

Some legal professionals described the cyber security obligations that Bill C-8 imposes on designated operators as "stringent and broad."[34] These compliance and operational oversight requirements – such as the development of cyber security programs, prompt disclosure of incidents and supply chain risk management – are perceived as significant, particularly for businesses with limited financial resources or technical capabilities.[35]

In addition, many legal professionals in the privacy and cyber security sectors remarked a lack of clarity in Bill C-8, including the classes of "designated operators," which are not defined,[36] and the broad scope of the new requirements to be defined later by regulation.[37] In their view, the lack of legislative clarity, combined with the power granted to the government to issue binding – and potentially confidential – cyber security directions, could impede the strategic planning of the operators concerned and undermine efficient implementation of their compliance measures.[38]

That said, other legal professionals welcomed the inclusion in the amended version of Bill C-8 of a statutory obligation for ministerial review within five years of Royal Assent. These observers considered this review mechanism an important legislative governance measure, because it enables assessing, based on real-world experience, whether the framework enacted is achieving its cyber security objectives and whether it is imposing proportionate constraints on designated operators.[39]

3.2 REPERCUSSIONS OF NEW OVERSIGHT POWERS: DIRECTIONS AND ORDERS

A number of legal professionals expressed concerns about the scope of the powers that Bill C-8 grants to regulatory agencies, including the power to conduct inspections, require internal audits and impose significant financial penalties, while recognizing that the bill is well intentioned and contains many necessary components.[40]

The concerns were heightened after the bill passed third reading. A number of legal professionals remarked on the House's rejection of certain amendments passed at the parliamentary committee stage that would have subjected some government orders to prior judicial approval.[41] According to these experts, this decision restored broad executive power while limiting oversight to judicial review after the fact.[42] These events highlighted the ongoing concerns of some commentators, who assert that the lack of prior judicial review has not been entirely corrected since 2025, despite the addition of some procedural mechanisms.

Some concerns were raised about the subjective standard set out in new section 15.4 of the *Telecommunications Act*. According to Matt Malone, a professor at the University of Ottawa Faculty of Law who specializes in privacy law and cyber security, this provision enables the Minister of Industry to "require any person," "within any time and subject to any conditions that the Minister may specify," to provide any information the minister believes is relevant to making an order or regulation.[43] This expert emphasized the subjective nature of this standard, which is based on the minister's discretion, with no explicit parameters regarding the nature of the information compelled or assurances about its use.[44] Other concerns pertained to the lack of provisions governing the reuse or subsequent disclosure of these data, including by CSE, in both Bill C-8 and its predecessor, Bill C-26.[45]

Moreover, Mr. Malone echoed the concerns the Citizen Lab expressed during consideration of Bill C-26 about the CCSPA's new powers to make secret directions.[46] It is worth noting that this power is not covered by the transparency measures normally required under the *Statutory Instruments Act*, which provides for the publication and review of regulations that could affect fundamental rights. According to these experts, this exemption could threaten Canadians' reasonable expectation of privacy while limiting democratic and judicial oversight of these powers.

That said, numerous witnesses heard during Bill C-8's consideration by the House of Commons Standing Committee on Public Safety and National Security (the Committee) made recommendations to strengthen the guardrails surrounding these new powers.

A number of them underscored the importance of including a clear and consistent standard requiring the exercise of these powers to be both necessary to achieve the desired objectives and proportional to the benefits achieved.[47] In this regard, the explicit inclusion of the necessity and proportionality criteria in multiple provisions of the amended version of Bill C-8 directly addresses those recommendations.

PRELIMINARY VERSION
UNEDITED

3.3 CONCERNS ABOUT PERSONAL AND CONFIDENTIAL INFORMATION

Legal experts in the area of data governance and cyber security expressed concerns about the protection of personal and confidential information under Bill C-8.[48] In their view, protecting this kind of information if a cyber security incident occurs could be challenging, given the new search and seizure powers granted to regulators, the record-keeping obligations for designated operators and the requirement to notify CSE and the appropriate regulator when a cyber security incident takes place.[49]

The Privacy Commissioner of Canada expressed support for the goal of strengthening the cyber security of critical infrastructure, but had reservations about the scope of the powers conferred on governments and regulatory bodies.[50] He also pointed to issues relating to compliance with section 8 of the Charter, owing to the powers that may authorize searches and seizures despite a lack of adequate safeguards and independent oversight mechanisms. While the Commissioner acknowledged some improvements compared with Bill C-26, he said that risks remained, particularly as regards the rules governing information sharing, including with foreign partners.

Similar concerns were raised by Mr. Malone about the compatibility of those powers with European personal data protection standards, and this difference could undermine European partners' trust and complicate cross-border cooperation in the sectors affected.[51]

In his Charter statement, the Minister of Justice recognized that some of the bill's provisions may infringe on Charter rights, including the right to privacy guaranteed by section 7 (right to life, liberty and security of the person) and section 8 (right to be secure against unreasonable government search or seizure). However, the statement concluded that these potential infringements are justifiable under section 1, given the objectives of national security and public safety and the legislative mechanisms that constrain the exercise of these powers.[52]

The Charter statement noted that the powers granted by Bill C-8 have explicit limits to prevent abuses, such as the prohibition on intercepting private communications, the duty to consider privacy impacts and the availability of parliamentary and judicial oversight mechanisms.[53]

3.4 LACK OF FINANCIAL AND TECHNICAL SUPPORT

Another point made is the lack of support measures, such as financial incentives, subsidies or technical resources, to help businesses comply with the new requirements.

PRELIMINARY VERSION
UNEDITED

For instance, Part 1 of Bill C-8 does not provide for any compensation for financial losses arising from TSPs' compliance with orders while imposing penalties of up to $15 million per day in case of non-compliance, which legal experts say amounts to a major financial burden on the private sector.[54] According to a senior associate in the privacy and cyber security group at a Toronto law firm, this shortcoming could impede the prompt and effective adoption of cyber security standards in a rapidly evolving threat environment.[55]

These concerns were raised again during the Committee's consideration of Bill C-8. Some witnesses recommended establishing a cyber security investment tax credit to encourage Canadian businesses to strengthen their internal capabilities and better comply with the new regulatory requirements.[56] Others suggested including a compensation mechanism allowing for the recovery of some of the costs imposed by government orders and creating a secure information disclosure process in order to reduce the operational and financial risks for affected businesses.[57]

Moreover, operators in the sectors affected by Part 2 of Bill C-8 face major compliance challenges. One of the main concerns relates to the high operational costs and substantial financial risk they will incur without compensation. During consideration of former Bill C-26, civil society experts pointed to problems with the costs of the reforms and the viability of small service providers in Canada.[58]

A lawyer in the privacy and data protection group at a Toronto law firm wrote that the new measures would create significant compliance problems for the telecommunications sector and critical federal infrastructure. These sectors should carry out strategic planning to avoid expensive enforcement actions and operational disruptions.[59]

3.5 REPERCUSSIONS ON CONTRACTUAL RELATIONS AND INDUSTRY

Bill C-8 could have downstream effects on contractual relations between regulated businesses and their suppliers. For example, section 15 of the CCSPA, enacted by clause 11 of Bill C-8, requires designated operators to "implement measures to address and reduce supply-chain risks identified by the cyber security program."[60] Experts, including an academic and legal professionals, say that enhanced cyber security requirements such as these could result in stricter contractual obligations that could put small or foreign suppliers at a disadvantage.[61]

In this regard, other legal professionals believe that "service providers should expect increasing cyber security standards from regulated customers, particularly when such services relate to critical cyber systems."[62]

PRELIMINARY VERSION
UNEDITED

NOTES

* This legislative summary is based in part on the legislative summary prepared by the Library of Parliament on Bill C-26, An Act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other Acts (44th Parliament, 1st Session).

1. Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 45th Parliament, 1st Session.
2. Bill C-8 passed second reading at the House of Commons on 3 October 2025 and was referred to the House of Commons Standing Committee on Public Safety and National Security (SECU), which considered it clause by clause. Following that review, the SECU reported the bill to the House with amendments on 11 March 2026.
3. Public Safety Canada, *Canada's National Cyber Security Strategy: Securing Canada's Digital Future*, January 2025.
4. Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 44th Parliament, 1st Session.
5. Public Safety Canada, *Canada's National Cyber Security Strategy: Securing Canada's Digital Future*, January 2025.
6. Ibid., p. 28.
7. Ibid.
8. Ibid., p. 3.
9. Catharine Tunney, "Senators amend error in cybersecurity bill that could have cancelled half of it," *CBC News*, 6 December 2024; quoted in Robbie Grant, *Bill C-26: A New Chapter in Canadian Cybersecurity Regulation*, McMillan LLP, 24 December 2024.
10. The 5G wireless network is the fifth generation of cellular communications technology, and it allows for a larger number of user devices, faster communication and higher speeds. See Communications Research Centre Canada, *What is 5G?* See also Innovation, Science and Economic Development Canada (ISED), *Statement from Minister Champagne on telecommunications security*, 19 May 2022; and ISED, *Policy Statement – Securing Canada's Telecommunications System*.
11. Sarah Lemelin-Bellerose, "5G Technology: Opportunities, Challenges and Risks," *HillNotes*, Library of Parliament, 13 February 2020; and United Kingdom, Department for Digital, Culture, Media & Sport, National Cyber Security Centre and the Rt. Hon. Oliver Dowden, *Huawei to be removed from UK 5G networks by 2027*, News release, 14 July 2020.
12. Australia, *Security of Critical Infrastructure Act 2018* (No. 29, 2018).
13. Australia, *Security Legislation Amendment (Critical Infrastructure) Act 2021*, (No. 124, 2021).
14. United States, *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Public Law 117-103, 117th Congress, 136 Stat. 49, Division Y in *Consolidated Appropriations Act, 2022*, H.R.2471.
15. United Kingdom, *The Network and Information Systems Regulations 2018*, 2018 No. 506.
16. European Union, EUR-Lex, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, in *Official Journal*, No. L 194.
17. Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 July 2025; and Hélène Deschamps Marquis et al., *Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know*, Borden Ladner Gervais LLP (BLG), 28 July 2025.
18. Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 July 2025.
19. Ibid.
20. Public Safety Canada, *Overview of the Proposed Changes to the* Telecommunications Act, Backgrounder.

PRELIMINARY VERSION
UNEDITED

21. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982*, 1982, c. 11 (U.K.).

22. *Criminal Code*, R.S.C. 1985, c. C-46.

23. For the purposes of this provision, a private communication includes a communication made in circumstances where its originator can reasonably expect that it will not be intercepted by a third party, including a radio-based telephone communication protected from intelligible reception. The term "intercept" encompasses listening to, recording and acquiring a communication or its content.

24. *Privacy Act*, R.S.C. 1985, c. P-21.

25. While the term "designated person" is not defined in the bill, new section 72.134 of the *Telecommunications Act* specifies that the minister may designate a person authorized to issue notices of violation or enter into compliance agreements. This person is then referred to as a "the designated person" or "the person who is designated to issue notices of violation" in new section 72.135, which sets out the procedure for those notices.

26. Depending on the economic sector of the designated operator, the "regulator" may be the Minister of Industry; the Minister of Transport; the Superintendent of Financial Institutions; the Bank of Canada; the Canadian Energy Regulator; or the Canadian Nuclear Safety Commission.

27. In the initial version of Bill C-26, section 17 of the Critical Cyber Systems Protection Act required designated operators to "immediately" report to CSE any cyber security incident involving their critical cyber systems.

28. *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76.

29. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

30. *Statutory Instruments Act*, R.S.C. 1985, c. S-22.

31. *Security of Canada Information Disclosure Act*, S.C. 2015, c. 20, s. 2.

32. For an analysis of existing legal definitions of "publicly available information" in Canadian privacy law, see Holly Porteous, "The Growing Importance of Open-Source Intelligence to National Security," *HillNotes*, Library of Parliament, 17 February 2022.

33. Department of Justice Canada, *Charter Statement on Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 23 September 2025.

34. Hélène Deschamps Marquis et al., *Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know*, BLG, 28 July 2025.

35. Ibid.; and Robbie Grant, *Back from the Grave: Bill C-8 Revives Comprehensive Cybersecurity Law*, McMillan LLP, 3 July 2025.

36. Molly Reynolds et al., *Government re-introduces cybersecurity bill for "vital" federal industries*, Torys LLP, 26 June 2025.

37. Hélène Deschamps Marquis et al., *Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know*, BLG, 28 July 2025.

38. Ibid.

39. Leslie Milton et al., *Bill C-8 Passes House of Commons Following Substantive Amendments and Speaker's Ruling*, Technology, Media, and Telecommunications Bulletin, Fasken Martineau DuMoulin LLP, 14 April 2026.

40. Hélène Deschamps Marquis et al., *Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know*, BLG, 28 July 2025; Molly Reynolds et al., *Government re-introduces cybersecurity bill for "vital" federal industries*, Torys LLP, 26 June 2025; Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 July 2025; and Matt Malone, "Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows?," *Balsillie Papers*, Vol. 7, No. 4, 23 July 2025.

41. House of Commons, *Debates*, 25 March 2026, 1605 (The Hon. Francis Scarpaleggia).

PRELIMINARY VERSION
UNEDITED

42. Leslie Milton et al., *Bill C-8 Passes House of Commons Following Substantive Amendments and Speaker's Ruling*, Technology, Media, and Telecommunications Bulletin, Fasken Martineau DuMoulin LLP, 14 April 2026.

43. Matt Malone, "Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows?," *Balsillie Papers*, Vol. 7, No. 4, 23 July 2025.

44. Anaïs Bussières McNicoll and Noa Mendelsohn Aviv, Canadian Civil Liberties Association, *Submission to the Standing Senate Committee on National Security, Defence and Veterans Affairs Regarding Bill C-26,* An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 13 November 2024. See also the submission of Matt Malone to the Standing Senate Committee on National Security, Defence and Veterans Affairs, following his testimony during consideration of Bill C-26.

45. Submission of Matt Malone to the Standing Senate Committee on National Security, Defence and Veterans Affairs, following his testimony during consideration of Bill C-26.

46. Ibid., quoting Kate Robertson, *Submission to the Senate Standing Committee on National Security, Defence and Veterans Affairs: Study of Bill C-26,* An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto, para. 35.

47. SECU, *Evidence*, Meeting 10, 30 October 2025, 1140 (Philippe Dufresne, Privacy Commissioner of Canada, Offices of the Information and Privacy Commissioners of Canada); *Evidence*, Meeting 10, 30 October 2025, 1235 (Luc Lefebvre, Chairman and Co-founder, Crypto Québec); *Evidence*, Meeting 10, 30 October 2025, 1240 (Sharon Polsky, President, Privacy and Access Council of Canada); and *Evidence*, Meeting 18, 4 December 2025, 1115 (Matthew Hatfield, Executive Director, OpenMedia).

48. Molly Reynolds et al., *Government re-introduces cybersecurity bill for "vital" federal industries*, Torys LLP, 26 June 2025.

49. Ibid.

50. Office of the Privacy Commissioner of Canada, "Issue sheets on Bill C-26," *Appearance before the Standing Committee on Public Safety and National Security of February 12, 2024*, 12 February 2024; and SECU, *Evidence*, Meeting 10, 30 October 2025, 1140 (Mr. Dufresne).

51. Matt Malone, "Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows?," *Balsillie Papers*, Vol. 7, No. 4, 23 July 2025.

52. Department of Justice Canada, *Charter Statement on Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 23 September 2025.

53. Ibid.

54. Hélène Deschamps Marquis *et al*., *Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know*, BLG, 28 July 2025; and Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 July 2025.

55. Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 July 2025.

56. SECU, *Evidence*, Meeting 10, 30 October 2025, 1230 (Aaron Shull, Managing Director and General Counsel, Centre for International Governance Innovation); and Aaron Shull, Centre for International Governance Innovation, *Bill C-8, An Act respecting cybersecurity amending the Telecommunications Act and making consequential amendments to other Acts*, Brief submitted to SECU, 8 December 2025.

57. Aaron Shull, Centre for International Governance Innovation, *Bill C-8, An Act respecting cybersecurity amending the Telecommunications Act and making consequential amendments to other Acts*, Brief submitted to SECU, 8 December 2025; and Canadian Telecommunications Association, *Bill C-8: An Act respecting cybersecurity amending the Telecommunications Act and making consequential amendments to other Acts*, Brief submitted to the House of Commons Standing Committee on Public Safety and National Security, 12 November 2025.

58. Kate Robertson, *Submission to the Senate Standing Committee on National Security, Defence and Veterans Affairs: Study of Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, Citizen Lab.

PRELIMINARY VERSION
UNEDITED

59. Robbie Grant, *Back from the Grave: Bill C-8 Revives Comprehensive Cybersecurity Law*, McMillan LLP, 3 July 2025.

60. Ibid.; and Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 July 2025.

61. Matt Malone, "Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows?," *Balsillie Papers*, Vol. 7, No. 4, 23 July 2025; and Robbie Grant, *Back from the Grave: Bill C-8 Revives Comprehensive Cybersecurity Law*, McMillan LLP, 3 July 2025.

62. Molly Reynolds et al., *Government re-introduces cybersecurity bill for "vital" federal industries*, Torys LLP, 26 June 2025.