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-26:
AN ACT RESPECTING CYBER SECURITY, AMENDING THE TELECOMMUNICATIONS ACT AND MAKING CONSEQUENTIAL AMENDMENTS TO OTHER ACTS

44-1-C26-E

6 October 2022

Jed Chong, Khamla Heminthavong and Holly Porteous

Parliamentary Information, Education and Research Services

AUTHORSHIP

6 October 2022	Jed Chong	Economics, Resources and International Affairs Division
	Khamla Heminthavong	Economics, Resources and International Affairs Division
	Holly Porteous	Legal and Social Affairs Division

ABOUT THIS PUBLICATION

Library of Parliament Legislative Summaries summarize bills currently before Parliament and provide background about them in an objective and impartial manner. They are prepared by Parliamentary Information, Education and Research Services, which carries out research for and provides information and analysis to parliamentarians and 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 House of Commons and Senate, 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 in this Library of Parliament Legislative Summary that have been made since the preceding issue are indicated in **bold print**.

Legislative Summary of Bill C-26
(Preliminary version)

44-1-C26-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-26: AN ACT RESPECTING CYBER SECURITY, AMENDING THE TELECOMMUNICATIONS ACT AND MAKING CONSEQUENTIAL AMENDMENTS TO OTHER ACTS

1 BACKGROUND

Bill C-26, An Act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other Acts, was introduced in the House of Commons by the Minister of Public Safety on 14 June 2022.[1]

This proposed legislation amends the *Telecommunications Act* and creates a new law, the Critical Cyber Systems Protection Act (CCSPA). The *Telecommunications Act* amendments empower the Governor in Council and the Minister of Industry to order Canadian telecommunications providers to undertake actions to secure the Canadian telecommunications system against a range of threats. These amendments follow the government's announcement that it intends to use these powers to prohibit the use of Huawei and ZTE products and services in Canada's telecommunications systems, particularly in 5G wireless networks.[2] The United States, United Kingdom, Australia and Japan have also banned Huawei from their 5G networks.[3]

The CCSPA (clause 13) establishes a cyber security compliance regime for federally regulated critical cyber infrastructure. The CCSPA appears to be patterned after Australia's *Security of Critical Infrastructure Act 2018*,[4] which was amended under the *Security Legislation Amendment (Critical Infrastructure) Act 2021*[5] to, among other things, significantly expand the Australian federal government's powers to enforce cyber security obligations for critical infrastructures and to intervene in the private sector's response to cyber incidents affecting critical infrastructures. Also of note is the United States' *Cyber Incident Reporting for Critical Infrastructure Act of 2022*,[6] which requires critical infrastructure operators to report cyber incidents to the Cybersecurity and Infrastructure Security Agency, and the United Kingdom's *The Network and Information Systems Regulations 2018*,[7] which were, in turn, derived from the European Union's 2016 Directive on security of network and information systems.[8] The overarching objective of all these regimes is to achieve an enhanced and common level of security for critical cyber infrastructures and to provide relevant authorities enhanced situational awareness.

2 DESCRIPTION AND ANALYSIS

2.1 PART 1: AMENDMENTS TO THE *TELECOMMUNICATIONS ACT*

Part 1 of the bill contains 12 clauses. Key clauses are discussed in the following sections.

2.1.1 Canadian Telecommunications Policy Objectives (Clause 1)

Clause 1 adds the promotion of the security of the telecommunications system to the policy objectives listed in section 7 of the *Telecommunications Act* (the Act). The addition allows the Minister of Industry and the Canadian Radio-television and Telecommunications Commission (CRTC) to consider this objective when exercising their respective powers under the Act. The same consideration is allowed under the *Radiocommunications Act* (the legislation governing spectrum allocation), which incorporates the Act's objectives by reference.[9]

2.1.2 Order-Making Powers (Clause 2)

Clause 2 adds sections 15.1 to 15.9 to the Act to give the federal government order making powers. Under new section 15.1, the Governor in Council may issue an order prohibiting a telecommunications service provider (TSP) from using the products and services of given suppliers if they are of the opinion that it is necessary to do so to secure the Canadian telecommunications system. The Governor in Council can also direct a TSP to remove all products provided by a specified supplier from its networks or facilities.

New section 15.2(1) gives the Minister of Industry the authority to make several types of orders. After consultation with the Minister of Public Safety, the Minister of Industry can issue an order obligating a TSP to stop providing services – or to pause the provision of services for a specified time period – to any person, including another TSP.

Under new section 15.2(2), the Minister of Industry can order a TSP to "do anything or refrain from doing anything" that is necessary, in the minister's opinion, to secure the Canadian telecommunications system. This new section contains a non-exhaustive list of examples illustrating how the minister may use this authority. Among other things, the Minister of Industry may issue an order to:

- direct a TSP to remove a specified product from 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.

The bill also specifies that no one is entitled to any compensation from the federal government for any financial losses resulting from these orders.

New section 15.4 allows the Minister of Industry to order any person to provide information required to implement the provisions of this legislation.

Although the bill requires the Governor in Council or Minister of Industry to publish these orders in the *Canada Gazette*, it also allows them to include provisions in these orders that prohibit the disclosure of its existence or some or all of its contents. New section 15.5(1) specifies that this authority can be used to prohibit the disclosure of trade secrets or economically sensitive data.

The Act currently has provisions allowing information sharing between the CRTC and Innovation, Science and Economic Development Canada. New section 15.6 broadens these provisions to include other ministers or agencies that may be involved in making an order, or in the investigation and enforcement activities related to an order.[10]

New section 15.7(1) allows the Minister of Industry to enter into an agreement to share any non-confidential information (i.e., trade secrets and economically sensitive data) collected under the Act with a provincial government, foreign state or international organization. The minister must believe that such information sharing is relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state.

Under new section 15.8(1), the Governor in Council can issue regulations covering anything that could otherwise be addressed in one of the ministerial orders.

New section 15.9 includes judicial review provisions. If an order from the Governor in Council or Minister of Industry is challenged in court, a judge can hear evidence and other information from the federal government that might be injurious to international relations, national defence, national security or endanger the safety of any person, without that information being disclosed to the public – including the applicant and its counsel.

The judge must provide the applicant with a summary of evidence and other information available to the judge that allows the applicant to be reasonably informed of the government's case. The summary must not include anything that, in the judge's opinion, would be injurious to international relations, national defence or national security or endanger the safety of any person if disclosed.

2.1.3 Inspection and Enforcement (Clauses 3 to 6)

Under clause 3, the CRTC is required to consider any orders from the Governor in Council or Minister of Industry when exercising its powers and duties as the regulator under the Act.

Clause 4 integrates the new order-making authorities from clause 2 into the existing Act's inspection and enforcement regime, allowing the Minister of Industry to designate inspectors to verify compliance or prevent non-compliance with any orders issued with the new order making authorities contained in this bill.

Under section 72(1) of the Act, a person who has incurred a loss or damage because of a contravention of the Act (or any decision or regulation made under the Act) can sue the person responsible for the contravention for an amount equal to the loss or damage. Section 72(3) of the Act includes exceptions to this civil liability regime. Clauses 5 amends section 72(3) of the Act so that the new order making authorities contained in this bill are part of this exemption from the civil liability regime.

Clause 6 amends section 72.001 to specify that the new order-making authorities contained in this bill are not subject to the Act's existing "General Administrative Monetary Penalties Scheme." As discussed below, the bill introduces a specific administrative monetary penalties system for violations of these new order-making authorities.

2.1.4 Administrative Monetary Penalties (Clause 7)

Under current sections 72.001 and 72.01of the *Telecommunications Act*, any individual who contravenes a provision of that Act or its regulations, whether for unsolicited telecommunications or non-compliance with a CRTC decision, for example, is liable to an administrative monetary penalty. Clause 7 adds an administrative monetary penalty scheme after section 72.13, under new sections 72.131 to 72.1393.

Clause 7 provides that the person who contravenes a provision, an order or a regulation (new sections 72.131 and 72.132) is liable to an administrative monetary penalty. It outlines penalties of up to $25,000 a day for an individual's first violation, or up to $50,000 for a subsequent contravention. For entities, the monetary penalties can be up to $10 million for a first violation, and for each day it continues. The amount can increase to $15 million for subsequent contraventions. Clause 7 also 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 their ability to pay the penalty (new section 72.133(1)). 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.

2.1.4.1 Designation of a Person or Class of Persons Authorized to Issue Notices of Violation, Their Content and Representations

Clause 7 outlines a procedure should new section 72.131 be contravened. The minister may designate a person or class of persons authorized to issue notices of violation (new section 72.134). They are authorized to cause a notice of violation to be served on a person they believe on reasonable grounds to have committed a violation (new section 72.135(1)).

Any notice of violation must name the person believed to have committed the violation, identify the violation and include the amount of the penalty for which the person is liable, as well as the time and manner of payment. It must also indicate that the person can pay the penalty immediately or make representations to the minister (new section 72.135(2)).

When a person served with a notice of violation makes representations to the minister, the minister must decide, on a balance of probabilities, whether or not the person committed the violation (new section 72.136(2)). Under new section 72.136(3), a person who is served with a notice of violation and neither pays the penalty nor

makes representations is deemed to have committed the violation. The minister may then impose the penalties set out in the notice.

2.1.4.2 Proceedings in Respect of a Violation, Commission of Violation by a Corporation, and Limitation Period or Prescription

Under new section 72.137, if a designated person offers to enter into a compliance agreement with the person believed to have committed the violation, the agreement is subject to any terms the designated person finds appropriate, including the reduction, in whole or in part, of the penalty set out in the notice of violation. It also provides that entering into a compliance agreement means the person is deemed to have committed the violation, and they may not make representations. If the designated person is of the opinion that the person who has entered into a compliance agreement has complied with it, they will put an end to the proceedings. If the agreement has not been complied with, the person who has entered into the compliance agreement will receive a notice of default informing them that they are liable to pay the amount set out in the initial notice of violation, within the time and in the manner set out in the notice.

When a corporation is believed to have committed a violation, its officers, directors or agents or mandatories are liable for the violation if they directed, authorized, assented to, acquiesced in or participated in the commission of a violation, whether or not the corporation is proceeded against (new section 72.138).

Any proceeding in respect of a violation may not be commenced later than three years after the day on which the subject matter of the proceeding becomes known to the minister (new section 72.1391(1)).

2.1.5 Provisions Common to Administrative Monetary Penalties Schemes

To encourage compliance, the bill relies on both an administrative monetary penalties scheme and a sentencing scheme. Like the administrative monetary penalties scheme, the sentencing scheme recognizes the personal responsibility of officers, directors or agents or mandatories who directed, authorized, assented to, acquiesced in or participated in the commission of an offence (clause 11).

2.1.5.1 Evidence and Defence

Anyone who contravenes an order or a regulation is guilty of an offence punishable on summary conviction and is liable either to a fine in an amount that is at the discretion of the court in the case of a corporation, or to imprisonment for a term of not more than two years less a day and/or to a fine in the case of an individual (new section 73(3.1).

Clause 9 amends section 72.14 to specify that, in a proceeding in respect of a violation, a notice or a decision appearing to be served is admissible as evidence without proof of the signature or official character of the person appearing to have signed it.

In most cases, it is a defence for a person in a proceeding in relation to a violation, under new section 73(3.4), to establish that the person exercised all due diligence to prevent the commission of the offence.

2.2 PART 2: THE CRITICAL CYBER SYSTEMS PROTECTION ACT

The CCSPA is set out at clause 13 of Bill C-26. Key provisions of the CCSPA are discussed in the following sections.

Respectively, sections 6 and 7 of the CCSPA empower the Governor in Council to order the addition of federally regulated "vital services and vital systems" to Schedule 1 of the Act and to add designated operators and regulators of these vital services and systems to Schedule 2 of the Act.

Schedule 1 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.

Being identified as a "designated operator" of a vital service or system under Schedule 2 creates a range of obligations. First and foremost is the obligation to establish a cyber security program within 90 days after becoming a member of a class of operators under Schedule 2.

2.2.1 Designated Operators Required to Establish and Maintain a Cyber Security Program

Section 9(1) of the CCSPA specifies what this cyber security program should achieve. These outcomes include:

- identification and management of any cyber risks to the organization, including supply chain risks and risks posed by third-party products and services;
- prevention of critical cyber system compromise;
- detection of any cyber security incidents that could affect or are affecting critical cyber systems; and
- limitation of damage in the event of a cyber security incident affecting critical cyber systems.

A "critical cyber system," it should be noted, is defined under section 2 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 act, omission or circumstance, that interferes or may interfere with" the continuity, security, 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. This interpretation is reinforced by section 12 of the CCSPA, which directs designated operators to maintain their cyber security program over time.

Section 10 of the CCSPA requires designated operators to immediately notify the "appropriate regulator[11]" that they have established a cyber security program and make this program available to the regulator within 90 days of their Schedule 2 designation. 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.

However, section 11 allows the regulator to extend the 90-day deadline one or more times for the purposes of enabling a designated operator to establish a cyber security program, or to make this program available to the regulator in the prescribed fashion, or both.

Section 12 of the CCSPA requires designated operators to not only implement their cyber security programs, but also to maintain them over time. The CCSPA sets out two mechanisms to ensure cyber security programs remain up to date: regulations and program reviews. While section 9(1)(e) requires designated operators to adhere to regulations, section 13 stipulates that designated operators review their cyber security programs at least once a year, completing this review within a 60-day timeframe, unless otherwise prescribed by regulation.

The designated operator must act on the review's findings, amending their cyber security program if necessary. Unless otherwise directed by the regulator, designated operators are required under section 13(3) to inform the regulator of whether or not they have made any changes to their program as a result of the program review within 30 days of the completion of that review.

Regulators are to be kept informed about other developments that could impact a designated operator's cyber security posture. Section 14 of the CCSPA directs designated operators to inform their regulators within 90 days of any material changes to:

- their ownership or control of a vital service or system;
- their supply chain or use of third-party service or product; and
- any circumstance prescribed by regulation.

Again, the regulator has discretion to extend this 90-day deadline one or more times.

Section 15 of the CCSPA requires supply chain and third-party cyber security risks to be treated with urgency. Designated operators must undertake reasonable steps, including those that may be prescribed through regulation, to mitigate these risks "as soon as" they are discovered. A regulator is authorized under section 16 to disclose any information, including confidential information[12], about a designated operator's cyber security program and section 15 risk mitigation measures to the Communications Security Establishment (CSE) to obtain CSE's "advice, guidance or services."

2.2.2 Mandatory Cyber Incident Reporting

The CCSPA imposes mandatory – possibly even automated[13] – cyber security incident reporting requirements on designated operators. Section 17 directs designated operators to "immediately" report to CSE any cyber security incident involving their critical cyber systems so that CSE can "exercise its powers or perform its duties and functions." Under section 18(b) of the *Communications Security Establishment Act* (CSE Act),[14] 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."

Of note, according to sections 17 and 18, designated operators are required to report a cyber security incident to CSE prior to notifying their regulator that an incident has occurred. Section 18(b) of the CCSPA further stipulates that designated operators only provide cyber security incident reports to their regulator "on request." Again, the timing and priority given to conveying incident-related information to CSE strongly suggests that the objective is to provide CSE with a nation-wide situational awareness that would enable it to defend vital systems and services if asked to do so.

Also of note, despite regulators having access to cyber security incident reporting under section 18(b), section 19 directs CSE to provide either a copy or a portion of incident reporting to the appropriate regulator upon request and for the purposes of verifying regulatory compliance or preventing non-compliance.

The CCSPA's inclusion of an additional means for regulators to obtain cyber security incident information likely reflects the possibility that CSE will learn of a cyber security incident from its own mandated activities and international intelligence sharing partnerships rather than the reporting of one or more designated operators. Further, some of this CSE-originated reporting may contain foreign intelligence or special operational information (i.e., sources and methods) that cannot be shared further.

2.2.3 Secret Cyber Security Directions

Sections 20 through 23 of the CCSPA empower the Governor in Council to issue secret orders called "cyber security directions" to designated operators. This secrecy is enabled by section 22(1), which exempts cyber security directions from sections 3, 5, and 11 of the *Statutory Instruments Act* (SIA).[15] Section 3 of the SIA requires proposed regulations to be examined by the Deputy Minister of Justice for, among other things, compliance with the *Canadian Charter of Rights and Freedoms*.[16] Section 5 of the SIA requires all regulations to be transmitted in both official languages to the Clerk of the Privy Council for registration and section 11 of the SIA requires all regulations to be published in the *Canada Gazette*, within 23 days of registration.

Under sections 24 and 25 of the CCSPA, designated operators that are subject to cyber security directions are prohibited from disclosing or allowing others to disclose the contents of these directions or even the fact that they have been issued, unless such disclosures are necessary to comply with the directives.

2.2.4 Federal Court Review

Section 145 of the CCSPA provides for a Federal Court review of cyber security directions. However, the Minister of Public Safety may request for such proceedings to be held in a closed court and for the applicant and the applicant's counsel to be provided with a summary of evidence rather than full disclosure of the government's case. If the judge accepts the government's argument that the disclosure of information or evidence in relation to the review could be injurious to international relations, national defence security or national security or endanger the safety of any person, the CCSPA requires the judge to protect the confidentiality of this information or evidence. Also of note, section 145(1)(e) indicates that the judge's decision may be based on evidence not provided to the applicant.

2.2.5 Information Disclosure Prohibitions and Permissions

Sections 26 through 29 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 section 26(1)(f)'s exception for disclosure under the *Security of Canada Information Disclosure Act*,[17] which enables information disclosures among 17 federal departments and agencies in order to protect Canada from "activities that undermine the security of Canada."

Of note, section 26(1)(b) creates an exception to the prohibition against disclosure for "publicly available information." At present, section 2 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 consumption, is accessible to the public on the global information infrastructure … or is available to the public on request, by subscription or by purchase."[18]

Section 27 of the CCSPA permits the Minister of Public Safety, responsible ministers and regulators to enter into 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.

2.2.6 Records to be Maintained, Generally Off-Site

Section 30 of the CCSPA requires designated operators to maintain records on 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 on any matter prescribed by the regulations.

Though the CCSPA does not provide explicit instruction on this matter, one expects that measures will be required to safeguard these records against unauthorized disclosure. Provisions in section 30(2) support this interpretation. This section requires designated operators to maintain their records within Canada, at a place and in a manner prescribed by regulations. In the absence of regulations, records are to be maintained at the designated operator's place of business.

2.2.7 Powers of the Regulators

Sections 32 to 85 of the CCSPA set out the respective powers of each of the six regulators assigned to oversee the operation of vital services and systems. For the purposes of verifying or preventing non-compliance with the CCSPA and its regulations, each of these six regulators are permitted under section 32 to enter any place – other than a dwelling-house – without consent or a warrant. Section 33(2) requires the regulator to obtain a warrant to enter a dwelling-house from a justice of the peace through an *ex parte* application.

Upon entry to a place, a regulator may examine, use or cause to be used any cyber system to, among other things, obtain information from it. The regulator can 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. Finally, 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.

2.2.8 Regulators May Order Mandatory Internal Audits

Under section 34 of the CCSPA and subject to any regulations, a regulator may issue a written order directing a designated operator to undertake an internal audit within a specified period of time to determine compliance with the CCSPA and its regulations. As these orders are exempt from the SIA, they are not published in the *Canada Gazette* and are therefore non-public.

Section 35 requires the designated operator to report the findings of its audit to the regulator. Where the designated operator has determined non-compliance, the designated operator's report to the regulator must identify the nature of the non-compliance and the measures the designated operator will undertake to achieve compliance.

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, section 36 empowers the regulator to order the designated operator to stop doing (or cause to be stopped) whatever is causing the designated operator (or likely will cause it) to be non-compliant, within a specified period of time. Likewise, the regulator can also order the designated operator to undertake measures to mitigate the effects of non-compliance. Again, under section 36(3), these compliance orders will not be made public.

Section 37 of the CCSPA states explicitly the mandatory nature of a compliance order and requires a designated operator subject to such an order to immediately notify the appropriate regulator when they have complied.

2.2.9 Compliance Order Review Requests

However, under section 38 of the CCSPA, a designated operator subject to a compliance order may submit a written request to the regulator to review the order. 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 its compliance order review, section 39 requires the regulator to confirm, amend, revoke or cancel the order, providing notice of this decision and reasons for it to the designated operator. Alternatively, if the regulator has not made a decision after 90 days of having received a review request or after any other time period that has been mutually agreed to by the regulator and designated operator, the regulator is deemed to have confirmed the original compliance order.

Section 146 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 of the report's completion.

NOTES

1. Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 44th Parliament, 1st Session. Please note that this legislative summary refers to the "Minister of Public Safety" rather than the "Minister of Public Safety and Emergency Preparedness" so as to reflect the current practice rather than the language of this department's 2005 creating statute – the *Department of Public Safety and Emergency Preparedness Act* – which remains unchanged.
2. 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*.
3. 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.
4. Australia, *Security of Critical Infrastructure Act 2018*, No. 29, 2018.
5. Australia, *Security Legislation Amendment (Critical Infrastructure) Act 2021*, No. 124, 2021.
6. United States, *Cyber Incident Reporting for Critical Infrastructure Act, 2022*, Public Law 117-103, 36 Stat. 49, Division Y in *Consolidated Appropriations Act, 2022*, H.R.2471.
7. United Kingdom, *The Network and Information Systems Regulations 2018*, 2018 No. 506.
8. 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*.
9. Public Safety Canada, *Overview of the Proposed Changes to the* Telecommunications Act, Backgrounder.

10. Ibid.

11. 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.

12. Section 2 of the Critical Cyber Security Systems Protection Act defines confidential information as any information that:

> (a) concerns a vulnerability of any designated operator's critical cyber system or the methods used to protect that system and that is consistently treated as confidential by the designated operator;
>
> (b) if disclosed 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; or
>
> (c) if disclosed could reasonably be expected to interfere with contractual or other negotiations of a designated operator.

13. Automated security information and event management (SIEM) tools have existed for decades. Nonetheless, it is possible that some designated operators are not using them or that the SIEM tools they are using would be incapable of providing Communications Security Establishment (CSE) specific incident-related information in a timely fashion. It is therefore noteworthy that Australia's *Security of Critical Infrastructure Act 2018* empowers its Secretary of the Department of Home Affairs to require a critical infrastructure operator to install and maintain system information software that collects and records system information to be transmitted to the Australian Signals Directorate (ASD). The ASD is CSE's Australian counterpart. Stakeholders identified this provision as being of greatest concern when it was first proposed in 2020. See Leah Ferris and Bernie Lai, *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*, Parliament of Australia, Parliamentary Library, Bills Digest No. 55, 2021–2022, 28 March 2020, p. 3.

14. *Communications Security Establishment Act*, (S.C. 2019, c. 13, s. 76)

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

16. *The Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act,1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

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

18. 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.