INTERNET INFRASTRUCTURE COALITION

Re: Senate Standing Committee on National Security, Defence and Veterans Affairs' study of Bill C-22, *An Act respecting lawful access*

Executive Summary

The Internet Infrastructure Coalition (i2Coalition) welcomes the opportunity to submit views to the Senate Standing Committee on National Security, Defence and Veterans Affairs on Bill C-22, the Lawful Access Act, 2026. We support timely, lawful access to information that electronic service providers already possess in order to facilitate law enforcement investigations. We also believe the security of all Canadians depends on secure Internet infrastructure operators; strong encryption that the law does not weaken, directly or indirectly; and regulatory stability for providers of key services underpinning the digital economy.

The House of Commons improved Part 2 of the bill, the Supporting Authorized Access to Information Act (SAAIA), by adding a limit on decryption obligations (s. 2(4)) and reducing the maximum metadata retention period to six months. While welcome improvements, the text before the Senate still contains many concerning items for Internet infrastructure operators.

The bill includes several elements that could be operationally onerous for our membership; allows for ongoing interference and weakening of end to end encryption as well as mandated decryption of any form of encryption that is not strictly end-to-end in nature; and leaves important obligations to future regulation and confidential orders. For the Internet infrastructure operators i2Coalition represents, these gaps create security risks and operational uncertainty—while eroding the rights of everyday Canadians. i2Coalition's members serve millions of Canadian individuals and businesses who entrust them with their data. This trust is rooted in the expectation that information will be accessed only when the law explicitly authorizes it, subject to meaningful oversight, and that the systems holding their data are built to keep others out. Part 2 puts this expectation at risk.

Our submission outlines the functional realities of compliance, points out enduring concerns about weakened encryption, and outlines the challenges of regulatory uncertainty for Internet infrastructure operators. We will address Part 2 of Bill C-22, which enacts the Supporting Authorized Access to Information Act. i2Coalition has serious concerns with Part 2, which are numerous and fundamental enough that Part 2 should be struck from the bill altogether. If the Committee does not choose to remove Part 2, we urge Senators to adopt the recommendations contained in this brief, which we consider the highest priority.

About i2Coalition

The Internet Infrastructure Coalition (i2Coalition) is a global trade association representing the interests of businesses[1] that build and operate essential layers of the Internet. i2Coalition membership, consisting of mostly small and medium-sized businesses, is international and includes companies operating in Canada for Canadians, as well as foreign companies providing services to Canadians. Members include cloud providers, data center operators, virtual private network (VPN) operators, domain name registrars, domain name registries, content delivery networks, web hosts, and other foundational Internet enterprises. Its mission is to preserve a free and open Internet as an engine for growth and innovation. i2Coalition works with members to advocate for sensible policies, establish and reinforce best practices, help create industry standards, and promote awareness of how the Internet works.

Weakening Encryption

i2Coalition closely monitors potential regulatory activity, which, though well intentioned, may have significant adverse effects for individual consumer privacy. In April 2026, i2Coalition published a report titled *Encryption at Risk.*[2] This document details how legislative and regulatory actions around the world are introducing systemic risks into encrypted systems—undermining security, user trust, and the foundational protections that enable digital commerce, privacy, and free expression.

The *Encryption at Risk* report examines policies such as client-side scanning mandates, lawful access requirements, and technical capability orders that compel providers to alter or undermine encryption systems. Drawing on global case studies from regions such as the European Union, United Kingdom, and Australia, the report highlights how these approaches introduce systemic weaknesses, even when framed as targeted or limited interventions. Many of the elements of Bill C-22, Part 2 fall in the category of *technical capability orders compelling providers to alter or undermine encryption systems.*

Decryption is described in section 2 of SAAIA as:

> Decryption
> (4) No obligations under this Act are to be construed as compelling an electronic service provider to decrypt, or to ensure that an authorized person is able to decrypt, any information that is encrypted by a person to whom the electronic service provider

[1] Internet Infrastructure Coalition, *Our Members,* https://i2coalition.com/membership/our-members
[2] Internet Infrastructure Coalition, *Encryption at Risk: How Weakening Secure Communications Undermines the Global Internet* (Q1 2026), https://policy.i2coalition.com/wp-content/uploads/2026/04/FINAL-Encryption-at-Risk-Report.pdf.

> provides services, unless the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information.

This prevents electronic service providers from being required to attempt decryption of the end-to-end encrypted communications of its users where the user is managing their own encryption keys. We say “attempt” because it is not possible for an outside party to decrypt end-to-end encrypted communications, even if the outside party is the service provider.

The definition of *decryption* in 2(4) does not prevent compelling a service provider to access data on an end-user’s device before data is encrypted and transmitted. For example, a cloud data backup provider could be required to gain access to a user’s device before data is encrypted and transmitted to the cloud provider’s servers. It also leaves open the possibility of ordering an electronic service provider to interfere with all other forms of encrypted communications where the service provider manages the keys. This inherently exposes the electronic service provider to systemic vulnerabilities.

Many of i2Coalition’s members employ forms of encryption where an end-user is not managing keys independently. This form of encryption, where the electronic service provider manages the keys, is employed as a matter of course in the operation of Internet infrastructure. It is a value-add—and often a non-negotiable one—for customers and it protects Internet infrastructure from bad actors. Transport layer security (TLS), for example, is a widely adopted protocol that can serve as a layer of protection for web applications, e-mail, remote work sessions via VPN, VoIP, and DNS resolution.

Sub-section 2(4) limits compelled decryption based on who provided the encryption and whether the provider possesses the information necessary to decrypt it. It does not limit orders that compel service providers to engineer other methods of interfering with encrypted communication. For example, the bill does not prevent the Minister from issuing an order compelling a service provider to architect a solution to turn *off* end-to-end encryption for certain users.

SAAIA addresses the issue of introducing systemic vulnerabilities as follows in sub-section 5(5):

> Systemic vulnerability
> (5) A core provider is not required to comply with a provision of a regulation made under subsection (2), with respect to an electronic service, if compliance with that provision would have the effect of requiring the provider to introduce a systemic vulnerability related to that service or of preventing the provider from rectifying such a vulnerability.
>
> For greater certainty

> (6) For greater certainty, subsection (2) does not authorize the making of regulations that confer an authority to access personal information about the persons to whom the core provider provides services.

However, the operational reality is that it is not possible to remove or weaken encryption for one person without creating a vulnerability that can be exploited against other users, or against the service infrastructure itself. To disable or create a bypass of encryption for a single user, a service provider must build a mechanism into its key management system and production code. This mechanism would also need to be hidden from its users and security auditors in a scenario where disclosure of information is limited by section 14 of SAAIA. The security vulnerabilities are a product of the mechanism existing, not of how often the mechanism is used. Further limitations on the powers of the Minister to interfere with the technical architecture of service providers are required. In simplest terms, there is no such thing as a back door that only the good guys can use.

Operational Exposure

As with other technical surveillance capability regimes, obligations under SAAIA are designed to facilitate the exercise of powers law enforcement and CSIS already have to obtain information, rather than creating new powers. Nothing in SAAIA can compel a service provider to disclose any customer information to CSIS or a law enforcement agency. This is a welcome division of powers and responsibilities.

Our primary concern with Part 2 is its scope. The SAAIA applies to “electronic service providers.” Read together with the definition of “electronic service,” this legislation reaches every organization that handles data in digital form. This captures not only the communications platforms that other technical surveillance regimes address, but also hosting companies, content delivery networks, domain registrars, domain registries, data centres, cloud operators, DDoS mitigation services, virtual private networks, cybersecurity service providers, and others whose purpose is to protect user data.

Under SAAIA, the Minister can issue orders to electronic service providers to collect and retain categories of metadata, with the exclusion of web browsing history, content, and social media activity. The same can be regulated by the Governor in Council for all core providers (currently undefined in the schedule) in a class. In practice, we note that many categories of metadata, including account and IP address records, connection and session times, routing and addressing information, and device or service identifiers can all be used to infer web browsing history, content, and social media activity even where these are not directly revealed.

Sub-section 5(2)(a) allows the Governor in Council to make regulations requiring core providers to build capabilities to extract and organize information that authorities are authorized to access, and provide it to them. Nothing in the provision limits this to information a provider already

collects or organizes, or prevents regulations from dictating how providers must structure the information. In practice, this means that core service providers will be responsible for architecting a ready-made system for responding to regulations, including collecting new data that it does not require for the regular delivery of a service. Electronic service providers could be forced to do the same under section 7, if ordered by the Minister. This contradicts the “Limiting Collection” principle in Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which directs companies to limit the collection of information to what is necessary for their purposes.[3]

The costs associated with developing information access systems can be substantial. In 2022 the Internet Corporation for Assigned Names and Numbers (ICANN) estimated the cost to develop a standardized system for access and disclosure (SSAD) for domain name registrars and registries at $20-27 million USD. The estimate for annual operating costs ranges from $14 million to $106 million USD. The wide variance in potential operating costs stems from unknown projected volumes for accreditation identification requests.[4]

In addition to the ability to require providers to generate new categories of data about their users to serve lawful access, core service providers can be regulated to install and report on the operation of “any device, equipment, or other thing” that may enable access to information in 5(2)(b). In practice, we are concerned that there are no limits or boundaries to this. This authority could cover hardware in a data centre, an agent running on servers, or code inside a production environment. This requires service providers to carry the burden of managing equipment or code they cannot fully inspect. Every new data store, extraction pathway, new device, equipment, or other thing is a new target for malicious actors. Access infrastructure built for lawful access regimes can be turned against the network it sits on.

A provider can only refuse to install a device, equipment, or other thing if it can show the equipment would introduce a "systemic vulnerability." However, this is difficult for a service provider to perform for a device it isn't permitted to fully inspect. Under s. 13, a provider must also help test this equipment, and the “systemic vulnerability” provision does not apply for testing purposes. Many of i2Coalition’s members operate global, multi-tenant infrastructure. In the case of cloud services, content delivery networks, and DNS services running on shared anycast infrastructure, a Canadian’s data could sit on the same path as foreign users, expanding the potential exposure plane beyond persons named in a warrant.

Obligations imposed under SAAIA could also threaten the adequacy status of Canada’s privacy laws under the EU GDPR, which would result in additional burdens for service providers who are operating highly integrated networks. A September letter from civil society organizations in

[3] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, sch 1, cl 4.4–4.4.1, https://lois-laws.justice.gc.ca/eng/acts/P-8.6/page-7.html.
[4] ICANN, *System for Standardized Access/Disclosure (SSAD) Operational Design Assessment* (January 25, 2022), 9, https://www.icann.org/en/system/files/files/ssad-oda-25jan22-en.pdf.

the European Union explicitly flags adequacy concerns.[5] A second September letter from the technology sector to the Minister of Public Safety and the Minister of Industry highlights the concerns of EU based businesses.[6]

Government equipment in a network, like any other third-party accommodation, makes the network less secure. Every device a service provider does not design or choose introduces vulnerabilities. Interception systems are known targets for bad actors, with many recent examples making headlines worldwide. The Salt Typhoon incident in 2024 involved state-sponsored hackers infiltrating US telecommunications companies, including Internet service providers. Reporting suggests that hackers targeted systems used to provide court-ordered access to communications systems for law enforcement and intelligence agencies.[7]

Finally, a “device, equipment, or other thing” can be placed where data transits provider infrastructure in the clear. For example, the decryption limit in 2(4) does not prevent collection of information at DNS resolvers, TLS termination points, or load balancers. Requiring service providers to provide government access to these areas would circumvent the protections for encryption contemplated in the earlier improvements made to the bill in the House of Commons.

Regulatory Uncertainty

The SAAIA sets up a framework for data collection and retention, but leaves most of the meaningful decisions to cabinet and to the Minister at a later stage. This regulatory uncertainty makes it difficult for service providers to plan or invest in continued provision of services to Canadian customers, or to provide Canadian customers with meaningful assurances regarding the privacy of their communications and data.

First, the term “core provider” remains undefined. Cabinet may add new classes by order without returning to Parliament. Obligations can also be imposed on any electronic service provider regardless of whether they are a core provider or not. The full suite of obligations is also undefined. Requirements for what providers must build, install, test, or retain will also be

[5] Access Now et al., “Open Letter from European Civil Society Organisations on Encryption and Privacy Threats in Canada’s Bill C-22,” letter to Ursula von der Leyen, President of the European Commission, Maroš Šefčovič, Michael McGrath, and Members of the European Parliament, September 14, 2026, Access Now, https://www.accessnow.org/press-release/encryption-and-privacy-threats-in-canadas-bill-c-22/.

[6] Association for Competitive Technology et al., “Joint Letter: Tech Industry Concerns with Bill C-22,” letter to Gary Anandasangaree, Minister of Public Safety, and Mélanie Joly, Minister of Industry, September 24, 2026, Chamber of Progress, https://progresschamber.org/wp-content/uploads/2026/09/Chamber-of-Progress_C-22_Joint-Letter_Tech-Industry-Concerns_Bill-C-22.pdf.

[7] Chris Jaikaran, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications*, CRS In Focus IF12798 (Washington, DC: Congressional Research Service (January 23, 2025), https://www.congress.gov/crs-product/IF12798.

set by later regulation or ministerial orders. Ministerial orders may also be secret and therefore unpublished. Because service providers will not be permitted to disclose their obligations in these situations, two providers of the same type of service may be subject to very different requirements without either one knowing.

Second, the systemic vulnerability exemption is dependent upon a “credible risk” under “international technical standards.” This is an important boundary. However, the bill gives no definition for these terms, and there is no dedicated process for resolving a systemic vulnerability dispute. Notably, if a service provider refuses to implement an obligation on the basis that it creates a systemic vulnerability, it exposes itself to compliance orders and severe penalties. The Act sets out the outcome to be avoided without establishing how a provider is meant to invoke it or how a disagreement about it will be resolved.

The Act does not specify which international technical standards apply or who selects them. It does not say what evidence a provider must produce to show that a requirement by the Governor in Council or the Minister would introduce a systemic vulnerability or who bears the burden of proof in those situations. It does not establish who decides whether the threshold has been met, whether that decision-maker must have technical expertise, or whether it is subject to an independent review.

Also absent is any safeguard for a provider that seeks to avoid a systemic vulnerability in good faith and is later found to be wrong from the regime’s significant non-compliance penalties. It also doesn’t provide a mechanism for reassessment when circumstances change. These gaps must be addressed because orders are subject to confidentiality obligations that limit a provider’s ability to seek outside technical advice or bring the dispute into public view. Service providers, especially smaller ones, will be forced to comply with requirements they believe to be unsafe rather than risk the substantial penalties. This is not a good scenario when sensitive information about Canadian customers is involved.

Bill C-22 creates an entire new class of regulated entities. Many of the small and medium-sized companies who could be impacted by C-22’s definition of “electronic service provider” have not operated in a regulated environment before. This regulatory uncertainty also creates a barrier for new Canadian entrants into the realm of electronic services. In a digital future driven by distributed computing, Canada surely does not want to create an environment where services offered within its borders are either too dangerous for citizens to use or too onerous for businesses to operate within compliance.

Recommendations

Our view is that Part 2 cannot be fixed by amendment alone, and the best course of action is to strike it from Bill C-22. If the Committee instead chooses to amend C-22, the priority recommendations set out in this submission are the minimum requirements to mitigate the

damage of authorized-access obligations on encryption, exposure of providers' systems, and regulatory uncertainty.

Encryption

1. Close the remaining gaps we've identified with respect to protection for encryption. Strong encryption protects the data of every Canadian. Providers and their customers need certainty that it cannot be undermined through regulations or secret orders. The committee should consider replacing section 2(4) with the following:

   Despite any other provision of this Act, nothing in this Act, or in any regulation, order, or request made under this Act, is to be interpreted as requiring an electronic service provider to

   (a)decrypt, or ensure that an authorized person is able to decrypt, any information that is encrypted;
   (b)remove, circumvent, or render less effective electronic protection including any method of encryption used in connection with its electronic service;
   (c)develop, maintain, or implement any capability to access information before it is encrypted or after it is decrypted, including on a user's device; or
   (d)refrain from offering any electronic service that uses end-to-end encryption.

Operational Exposure

1. Narrow the definition of "electronic service provider" to confine it to those companies that offer communication services directly to end-users. At a minimum, the Committee should add a clause excluding providers, *to the extent that they offer the following services:*
   a. Internet infrastructure services where the provider does not offer communications services to end users, such as domain name registration and resolution, hosting, cloud infrastructure, content delivery networks, virtual private networks, or interconnection and transit points;
   b. cybersecurity services, such as those which detect, prevent, mitigate, or respond to threats to the security of information, networks, or systems;
   c. the encryption, authentication, or protection of information.

2. Prevent the Governor in Council or the Minister from making regulations or orders that could require core providers to architect systems to collect new data. Limit metadata collection and provision in 5(2) to information that providers already collect and possess in their operations. i2Coalition recommends that the Committee amend section 5(2)(a) as follows:

(a) the development, implementation, assessment, testing and maintenance of operational and technical capabilities, including capabilities related to extracting and organizing information that is authorized to be accessed and that the core provider collects, generates or retains in the ordinary course of providing the electronic service, and to providing access to such information to authorized persons;

and add the following subsection:

For greater certainty, regulations made under paragraph (2)(a) may not require a core provider to collect, generate or retain information that it does not otherwise collect, generate or retain in the ordinary course of providing the electronic service, or change the manner in which it stores or organizes information within its systems. Any requirement respecting the format of information applies only to the manner in which information is provided to authorized persons.

Regulatory Uncertainty

1. Establish a clear, fair process for systemic vulnerability determinations. We recommend that the Committee amends Part 2 to require that:
    a. The standards and evidentiary requirements for assessing systemic vulnerabilities be published so that service providers and the government are evaluating claims against the same standards;
    b. Where a service provider gives notice, with justification, that a requirement would introduce a systemic vulnerability, the obligation to comply will be suspended until the claim is determined, and no penalty applies for non-compliance during that period;
    c. The burden rests on the government to demonstrate that a requirement would not introduce a systemic vulnerability;
    d. Disputed claims be referred to an independent reviewer with technical expertise, whose determinations are subject to review; and
    e. Providers be able to seek reassessment of an earlier determination when new vulnerabilities, threats, or changes to their systems emerge.

Conclusion

i2Coalition recognizes the legitimate needs of law enforcement and national security agencies, and supports timely access to information that service providers already possess under the appropriate legal authority, with independent oversight. The House of Commons has made meaningful improvements to Part 2. However, those improvements do not resolve its fundamental problems, and the Senate now has the opportunity to ensure that the framework does not undermine the security it is meant to support.

The stakes for Canadians are high, and for Canadian Internet infrastructure operators they are existential. If the SAAIA allows encryption to be circumvented, or if its key elements are left to undefined regulations and confidential orders, then providers will face two choices: offer Canadians services with weaker privacy and security protections, or withdraw from the Canadian market. This is particularly challenging for companies domiciled in Canada, and both outcomes cause harm to Canadians.

The first exposes their data to the same malicious actors that strong cybersecurity measures exist to keep out. The second leaves Canadians with fewer choices and fewer of the secure online services they rely on. This is not a hypothetical situation. As documented in our *Encryption at Risk* report, Apple withdrew its most secure cloud backup service from users in the United Kingdom after a technical capability notice, and several global VPN providers withdrew their services from India rather than comply with logging mandates that were incompatible with their security procedures. Small service providers, which make up most of the i2Coalition's membership, have the least capacity to absorb compliance costs or legal risk, and are the most likely to conclude that serving Canadian customers is no longer viable.

These outcomes are avoidable. The problems with Part 2 are numerous and fundamental enough that i2Coalition believes the most effective remedy is to strike Part 2 from Bill C-22 altogether. Should the Committee choose instead to amend the proposed legislation, the priority amendments recommended in this submission are essential: improve the protections for encryption, confine the Act to the providers it is designed to address, limit obligations to information providers already hold, and give providers a process for raising security concerns.

i2Coalition thanks the Committee for its consideration and welcomes the opportunity to discuss these recommendations further.