Bill C-22: Secure infrastructure and lawful access

Written submission to the Standing Senate Committee on National Security, Defence and Veterans Affairs

Submitted by Tailscale | November 6, 2026

Co-authored by Avery Pennarun, co-founder and CEO, and Will Moore, Head of Policy & Public Affairs, Sovereign AI.

Executive summary and position

[1] Tailscale is a Canadian-founded technology company that provides secure, identity-aware networking for individuals, businesses and public-sector organizations. We support lawful, targeted investigations and respond to valid legal requests for information in our possession or control. We also design our systems to avoid collecting information we do not need. Those principles should reinforce each other.

[2] Today, more than 50,000 businesses, and millions of individuals worldwide use Tailscale. We are a fully remote company with over 300 employees across Canada and internationally. In October 2026, we announced a multi-million-dollar, multi-year investment in sovereign AI, focused on giving organizations greater control over their technology and infrastructure. We have a direct interest in ensuring Canada remains a place where companies can build secure, innovative products that compete globally.

[3] We welcome the amendments made to Bill C-22 in the House of Commons, including the reduction of the proposed metadata retention limit from 12 to six months, the condition that retained metadata categories be essential, and explicit protections related to decryption and systemic vulnerabilities. These are substantive improvements.

[4] We remain concerned about Part 2, which would enact the Supporting Authorized Access to Information Act. Sections 5 and 7 would permit regulations and provider-specific orders requiring technical capabilities, equipment and metadata retention. The precise duties would depend on later regulations or orders. The law should limit those powers now, rather than rely on future decision-makers to avoid harmful designs.

[5] Tailscale supports the objective of enabling legitimate, duly authorized access. We cannot support Part 2 in its present form without stronger limits on compelled collection, changes to secure architecture, and confidential technical obligations.

Recommendations at a glance

[6] **Require technical obligations to be necessary and proportionate.** Amend sections 5 and 7 to require evidence that proposed obligations are justified, technically feasible, and cannot reasonably be achieved through less intrusive means.

[7] **Limit mandatory collection and retention of metadata.** Amend section 5, including subsection 5(4), and section 7 to prevent providers from being required to collect new categories of information solely for future investigations or redesign products to enable such collection.

[8] **Protect existing security architecture.** Strengthen sections 2, 5, 7 and 24 to explicitly protect devices, software, equipment and operating systems, and prohibit requirements to weaken encryption or introduce new interception capabilities before information is encrypted.

[9] **Recognize differences between technology providers.** Require technical obligations to reflect how a provider's service operates, what information it can access, and whether compliance would require fundamental changes to its security design.

[10] **Introduce independent technical review.** Allow providers to challenge requirements that could introduce security risks, with an independent technical assessment before disputed changes must be implemented.

[11] **Improve transparency and security reporting.** Allow providers to publish aggregate information about government-imposed obligations and disclose security risks, while protecting the confidentiality of ongoing investigations.

1. Why network architecture matters

[12] Not all Virtual Private Networks (VPNs) work the same way.

[13] Many consumer VPN services, particularly those marketed for privacy or anonymity, work by routing a user's internet traffic through a server operated by the VPN provider. The provider sits between the user and the websites or services they access. Depending on how the service operates, the provider may have access to information about those connections.

[14] Tailscale and other similar services work differently. Rather than routing internet traffic through Tailscale's servers, our software allows devices to establish secure, private connections directly with one another. Tailscale helps those devices find each other and establish the connection, but the communication itself normally travels directly between them.

[15] This approach is called peer-to-peer networking. It reduces the need for central servers to handle people's communications and limits the information available to Tailscale. When a direct connection is not possible, communications remain encrypted.

[16] Tailscale can provide information it holds in response to lawful requests, as we do today. But requiring us to collect information that doesn't normally pass through our systems could mean fundamentally changing how our technology works.

[17] Bill C-22 should recognize how different networking technologies operate, rather than assume all VPN providers have the same access to their users' communications.

2. The amendments are welcome, but concerns remain

[18] We welcome the amendments made by the House of Commons, particularly the stronger protections for encryption, restrictions on introducing systemic vulnerabilities, and limits on metadata retention.

[19] However, these changes do not fully address our concerns about the technical requirements that could be imposed on providers. A company could still be required to develop or maintain capabilities to collect information it does not currently possess. For companies like Tailscale, this could mean redesigning systems that were deliberately built to minimize the information they collect.

[20] The protections against systemic vulnerabilities are also limited in scope. They do not expressly cover every component involved in securing communications, including customer devices and operating systems. Some requirements could also be imposed through confidential ministerial orders, making it difficult for providers and customers to understand changes that could affect their security.

We believe the legislation should explicitly protect companies from being required to weaken or fundamentally redesign secure systems to facilitate access to information they do not ordinarily collect.

3. Recommended amendments

1. Require technical obligations to be necessary and proportionate

Relevant provisions: Sections 5(3) and 7(3)

[21] Bill C-22 requires the government to consider factors such as cost, technical feasibility, privacy and cybersecurity when imposing obligations on providers. However, it does not require the government to demonstrate that those obligations are necessary and proportionate to the intended outcome.

[22] We recommend amending the bill to require evidence that a proposed obligation is necessary, that its benefits justify its impact on security and privacy, and that less intrusive alternatives have been considered.

[23] There is a considerable difference between asking a company to provide records it already holds and requiring it to build new monitoring capabilities for possible future investigations. Both the Privacy Commissioner and the Intelligence Commissioner recommended stronger proportionality requirements in their testimony to this Committee on November 2, 2026.

2. Do not require companies to collect information they would not otherwise hold

Relevant provisions: Sections 5(2), 5(4) and 7(1)

[24] The House of Commons reduced the maximum metadata retention period to six months. This is an improvement, but it does not fully address what information companies could be required to collect in the first place.

[25] For a company like Tailscale, complying with new metadata requirements could mean changing its software to record information it does not ordinarily collect, then building systems to store and protect that information. Every new collection system creates additional security responsibilities and another potential target for attackers.

[26] Section 5(4) currently restricts certain categories of information that providers can be required to retain. We recommend expanding these protections to explicitly prohibit regulations from requiring providers to redesign their products to collect or retain information beyond their ordinary operational needs. The same restriction should apply to technical-capability requirements under sections 5(2)(a) and (b), and to ministerial orders under section 7.

[27] **Mandatory retention should be limited to clearly defined information that providers already generate through normal operations.** The law should preserve the ability of investigators to require preservation of specific information through existing lawful processes, without requiring companies to build permanent collection capabilities for possible future investigations.

3. Protect the security of the entire system, not only encryption

Relevant provisions: Sections 2(1), 2(4), 5(5), 7(5) and 24(2.1)

[28] We welcome the bill's protections for encryption and against the introduction of systemic vulnerabilities. However, secure communications depend on more than encryption alone. They also depend on how software handles encryption keys, authenticates devices and limits access to information.

[29] Tailscale's software runs directly on customer devices to establish secure connections. A requirement to modify that software to capture information before encryption, change how devices authenticate or introduce new access mechanisms could weaken security without explicitly requiring the company to decrypt communications.

[30] Section 2(1) currently defines a systemic vulnerability in relation to the electronic protections of an "electronic service." This may leave uncertainty about protections for devices, equipment, software and operating systems. We recommend expanding the definition to expressly include these components. A security weakness introduced on a customer's device should receive the same protection as one introduced into a provider's central systems.

This approach is also supported by the Chamber of Progress, which recommended extending the definition of systemic vulnerability to cover devices, equipment and operating systems in its submission to this Committee.

[31] We also recommend strengthening section 2(4) to make clear that lawful access obligations cannot compel providers to redesign products, alter security configurations or build capabilities to intercept information before encryption. The existing protection against compelled decryption should not be bypassed by requiring a provider to change where or how information is collected.

[32] The definition of systemic vulnerability should also protect against risks that extend beyond the person subject to an investigation. A technical capability introduced for one authorized investigation may create a weakness in software used by many customers. A warrant limits who investigators may lawfully investigate, but it does not necessarily limit who could be affected by a software vulnerability.

4. Recognize that different technology providers operate differently

Relevant provisions: Sections 2(1), 5(1), 7(1) and 48

[33] Bill C-22 defines electronic service providers broadly. It allows the government to establish obligations for classes of providers and to issue orders to individual companies.

[34] However, companies providing similar services may use fundamentally different technologies. As explained earlier, some VPN providers route customer traffic through central servers, while Tailscale primarily connects devices directly. These different designs determine what information a provider can access and what it can reasonably be expected to supply.

[35] The bill already permits different requirements for different classes of providers, but it does not require obligations to reflect these technical differences. We recommend requiring the government to consider how a provider's service operates, what information it possesses or controls, and whether compliance would require changes to its underlying security design.

Providers should not face identical technical obligations simply because their products fall under the same broad definition.

5. Allow independent technical review before changes are required

Relevant provisions: Sections 7 to 9, 13 and 24 to 26

[36] Bill C-22 includes oversight measures, including review of ministerial orders by the Intelligence Commissioner and an opportunity for providers to make representations. These are welcome safeguards.

[37] However, providers should also have a clear way to challenge requirements that they believe would introduce security risks, before those changes must be implemented. The existing oversight process does not expressly guarantee an independent engineering assessment of the effects on a provider's systems.

[38] We recommend establishing a process through which a provider can request an independent assessment by qualified technical experts. The assessment should examine whether the proposed requirement is technically feasible, whether it would weaken security, and whether a safer alternative could achieve the same result.

[39] Except in narrowly defined urgent circumstances, implementation of the disputed requirement should be paused until that assessment is completed. The process should also apply where testing or assessment of equipment under section 13 could create security risks. The Privacy Commissioner recommended a similar independent assessment mechanism during his November 2 appearance before the Committee.

6. Allow companies to report security risks without compromising investigations

Relevant provisions: Sections 14, 15 and 49

[40] We recognize that some government requests must remain confidential to protect ongoing investigations. Bill C-22 already provides for annual government reporting and permits certain disclosures to regulatory authorities.

[41] However, these provisions do not expressly give companies the ability to report aggregate information about technical obligations imposed on their services. We recommend allowing providers to publish delayed, aggregate information about the orders and requirements they receive, without identifying individuals or disclosing details of investigations.

[42] The legislation should also provide a clear process for companies to notify affected customers and appropriate security experts when a technical requirement creates a security concern. Necessary confidentiality protections should remain in place, but they should not prevent a company from addressing a security risk that could affect its customers.

Conclusion

[43] Canada has an opportunity to improve lawful access while protecting the security of the technology Canadians depend on. The amendments already made to Bill C-22 show that these objectives can be pursued together. The remaining concerns can be addressed through clearer limits on technical obligations, stronger protections for existing security architectures, and independent review before potentially harmful changes are imposed.

[44] Tailscale respectfully requests the opportunity to appear before the Standing Senate Committee on National Security, Defence and Veterans Affairs in connection with its study of Bill C-22. Our co-founder and CEO, Avery Pennarun, would welcome the opportunity to explain the technical implications of the proposed legislation and answer senators' questions.

Selected sources

1. **Parliament of Canada.** Bill C-22, Lawful Access Act, 2026, as passed by the House of Commons, June 18, 2026. Particularly Part 2, the proposed Supporting Authorized Access to Information Act, sections 2, 5, 7 to 9, 13 to 15, 24 to 26, 48 and 49.
2. **Office of the Privacy Commissioner of Canada.** Statement to the Standing Senate Committee on National Security, Defence and Veterans Affairs, November 2, 2026. Recommendations on necessity, proportionality and independent technical review.
3. **Office of the Intelligence Commissioner.** Remarks to the Standing Senate Committee on National Security, Defence and Veterans Affairs, November 2, 2026. Recommendation to strengthen the proportionality test for ministerial orders under section 7(3).
4. **Canadian Centre for Cyber Security.** Virtual private networks (ITSAP.80.101). Government guidance explaining different VPN architectures and their security considerations.
5. **Tailscale.** Connection types. Technical explanation of direct peer-to-peer connections and encrypted relayed connections.
6. **Tailscale.** Tailscale encryption. Explanation of end-to-end encryption and encryption key handling.
7. **Tailscale.** Network flow logs. Documentation of network flow logging, retention and limitations on verifying client-reported information.
8. **Avery Pennarun.** Canada's Bill C-22 and the security cost of collecting more data, May 26, 2026. Tailscale's original public position, based on the bill before the House amendments.
9. **Tailscale.** Company overview and Tailscale careers. Information on Tailscale's global workforce and remote-first operations.
10. **Tailscale.** Tailscale homepage. Publicly reported business customer count of more than 50,000.
11. **Avery Pennarun.** Sovereign AI starts with open infrastructure, October 13, 2026. Announcement of Tailscale's multi-million-dollar, multi-year investment in sovereign AI.
12. **Chamber of Progress.** Written submission to the Standing Senate Committee on National Security, Defence and Veterans Affairs concerning Bill C-22, October 2026. Proposed amendments addressing encryption, systemic vulnerabilities affecting devices and operating systems, metadata retention and transparency.