

October 26, 2026

Decrypting Bill C-22, Part III: Backdoors by Another Name: The Limits of C-22's Systemic Vulnerability Safeguard

By: Alexandra Lyn, Joel Reardon, and Michael Nesbitt

Legislation Commented On: [Bill C-22, *An Act respecting lawful access*, 1st Sess, 45th Parl, 2026 \(as passed by the House of Commons 18 June 2026\)](#)

Status: As of this writing, Bill C-22 has passed the House of Commons and remains at second reading in the Senate, where debate most recently resumed on 8 October 2026 ([LEGISinfo, Bill C-22 \(45-1\)](#)).

This is the third post in our four-part series translating the ongoing debate on Bill C-22, *An Act respecting lawful access*, for non-technical and non-legal readers. By way of reminder, lawful access refers to law enforcement's legal powers to conduct searches and seizures of private spaces and information—think searches of your home (spaces) or your computer or browsing history (information)—for investigative purposes. Bill C-22 is the government's controversial attempt to update Canada's lawful access regime by granting police broad new powers of search and seizure.

For interested readers, our [first post](#) provided a more detailed introduction to the Bill and its legal background. Our [second post](#) examined the Bill's mandatory metadata retention regime. This third blog post tackles perhaps the most controversial aspect of the Bill, that being the power to enable the state to force electronic service providers (ESPs) to weaken encryption and other cryptographic protections in furtherance of its lawful access ambitions and, relatedly, the inadequacy of the Bill's safeguard against “systemic vulnerabilities”.

Indeed, since its introduction, privacy advocates, civil liberties organizations, and industry stakeholders have warned that this power to compel the weakening of encryption would, contrary to the government's goals, leave Canadians' data exposed, not just to the state, but also to malicious actors who would be quick to exploit any weakness created for lawful access (see e.g., Robert Diab, “[Parliament Has Amended Bill C-22, But Has It Addressed the Biggest Privacy Concerns?](#)” (19 June 2026), online (blog): *Robert Diab*; Michael , “[Years of Uncertainty: Bill C-22's Missing Regulations and Secret Ministerial Orders](#)” (14 October 2026), online (blog): *Michael Geist*). These concerns stem from the means by which the government intends to facilitate its expanded lawful access powers under C-22, which it sets out in Part 2 of the Bill, the *Supporting Authorized Access to Information Act* (the *SAAIA* or the *Act*).

To make a long story short, the *SAAILA* authorizes the Governor in Council to make regulations requiring “core providers” to develop and maintain “operational and technical capabilities” that allow authorized persons to access information, and to install and operate “any device, equipment or other thing” for the same purpose (*SAAILA*, s 5(2)(a), (b)). The Minister may impose the same obligations on any ESP by order, “whether or not the provider is a core provider”, and may require any ESP to assist in testing lawful access tools (*SAAILA*, ss 7(1), 13(1)). In other words, the *SAAILA* may require ESPs to build or implement into their own systems a means for the state to access Canadians’ data.

The concern, therefore, is that by requiring ESPs to embed mechanisms for state access to data, the state will expose Canadians’ data not only to the government but also to bad actors. This concern is neither speculative nor overstated. Security experts have long warned that any mechanism designed to give the state exceptional access to secure systems creates a vulnerability that others can exploit (Harold Abelson et al, “[Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications](#)” (2015) 1:1 J Cybersecurity 69 at 70, 75). These mechanisms built to give the state access to the data of a particular person of interest will also undermine the security for every person who uses the service.

This concern is far-reaching. As we discussed in our [first post](#), the definition of an ESP is exceptionally broad. Although it is easy to picture ESPs as large corporations such as Meta, Apple, Google, Rogers or Bell, the definition can also capture the smaller developers and open-source projects on which much of the Internet’s security infrastructure depends. In principle, then, there is almost no limit to the digital infrastructure into which the *SAAILA* could require such mechanisms to be embedded, and in which the resulting vulnerabilities could manifest.

Through a series of amendments in June 2026, the government sought to assuage some of these concerns by revising the definition of “systemic vulnerability” (*SAAILA*, s 2(1)) and adding an express decryption provision (*SAAILA*, s 2(4)). These amendments also extended the systemic vulnerability exemption to compliance orders, and ensured that an ESP’s duty to comply with an order does not override that exemption (*SAAILA*, ss 11, 24(2.1), 25(1)). While regulations and orders under sections 5 and 7 of the *SAAILA* were already subject to a systemic vulnerability exemption, the amendments modified its wording, so that an ESP is now excused where compliance “would have the effect of requiring” it to introduce a systemic vulnerability, rather than only where compliance “would require” it (*SAAILA*, ss 5(5), 7(5); [Bill C-22, An Act respecting lawful access, 1st Sess, 45th Parl, 2026, cl 41](#) (first reading 12 March 2026)) (Bill C-22, first reading).

Despite these safeguards, the systemic vulnerability framework leaves significant gaps. As we discuss below, the decryption provision may protect end-to-end encryption, but it offers little assurance for the encryption Canadians rely on every time they use the web. It could therefore permit requirements that expose not merely which websites Canadians visit, but the full content of those visits, compounding the risks of the metadata retention regime examined in our [second post](#). The framework remains limited in scope, uncertain in application, and structured in a manner that offloads onto ESPs the dual burden of facilitating lawful access and advocating for Canadians’ digital security. Put differently, the systemic vulnerability framework in the *SAAILA* reflects an unrealistic government aspiration, divorced from technical reality, which it foists onto ESPs to achieve on its behalf.

In this post, we first set out the Bill’s definition of “systemic vulnerability”, which has three components: two elements and one exception. A vulnerability qualifies only if (1) it exists in the “electronic protections” of an electronic service; (2) it creates a “credible risk”, based on “recognized international technical standards”, that secure information could be accessed without authority; and (3) the risk does not relate only to the targets of a lawful authorization. We then examine each component in turn, identifying the gaps in its drafting and the uncertainty these gaps create for the scope of protection under the systemic vulnerability framework. The scope of this framework, at the threshold level, turns on which cryptographic protections qualify as “electronic protections”. Our discussion of the first component therefore includes a brief primer on cryptography. In that primer, we explain how encryption and other cryptographic tools work, how the decryption provision in section 2(4) applies to each, and why security experts warn against “back doors”. Second, we turn to a structural limitation of the Bill’s framework: the safeguard does not stop the government from imposing requirements that would create systemic vulnerabilities; rather, it only permits an ESP to refuse to comply. We also consider the practical consequences of that structure, which places the burden of identifying and resisting systemic vulnerabilities on ESPs, rather than on the government. Third, we examine the obligation to assist in testing under section 13 of the *SAAILA*, which contains no systemic vulnerability exemption and extends to virtually any ESP in Canada. Fourth and finally, we consolidate the proposed amendments set out throughout the post into a single section for ease of reference.

Where we propose amendments to the *SAAILA*, additions are underlined, deletions are struck through, and ellipses indicate unchanged text that has been omitted. We offer these amendments with some degree of caution. Legislative drafting involves policy choices and technical considerations beyond the scope of this post, and we do not suggest that our proposed language should be adopted wholesale. Rather, we offer them as illustrations of how Parliament might address the concerns that we identify, and as a starting point for further consideration of potential amendments to the *SAAILA*.

We also wish to clarify the terminology used in this post. The term “systemic vulnerability” has been defined by the legislature in section 2(1) of the *SAAILA* and it has a particular (albeit unclear) legislative meaning. The term “vulnerability” is a term of art in computer science, which generally means a “[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source” (US, National Institute of Standards and Technology, Computer Security Resource Center, “[Glossary: vulnerability](#)”). As we discuss in the post that follows, these two terms are not synonymous in meaning. Indeed, the term “systemic vulnerability” as used in the *SAAILA* is considerably narrower than the concept of “vulnerability” in computer science. Accordingly, we use the term “systemic vulnerability” only in reference to the *SAAILA*, and the term “vulnerability” or sometimes “security vulnerability” when discussing security weaknesses more generally. We often do the latter because these vulnerabilities exist, and present real risks, irrespective of whether the *SAAILA* classifies them as “systemic vulnerabilities” falling within the scope of the *Act*.

1. Systemic Vulnerability: Its Legislative History, Legislative Definition, and the Gaps That Remain

The *SAIA* addresses data security principally through a systemic vulnerability framework, supplemented by an express decryption provision. Section 2(1) of the *SAIA* defines “systemic vulnerability” as:

[a] vulnerability in the electronic protections of an electronic service that creates a credible risk, based on recognized international technical standards, that secure information could be accessed by a person who does not have any right or authority to do so, other than a risk that relates only to information related to persons with respect to whom a warrant, order or other authority to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act* — or any similar authority conferred under another Act of Parliament — applies. (*SAIA*, s 2(1))

The definition has three component parts: two elements and one exception. A vulnerability qualifies as a “systemic vulnerability” only if:

1. **It exists in an electronic protection.** The vulnerability must be “in the electronic protections of an electronic service”, such as its authentication or encryption.
2. **It creates a credible risk of unauthorized access.** The vulnerability must create a credible risk, measured against “recognized international technical standards”, that someone without lawful authority could access secure information.
3. **Risks confined to lawful targets are excluded.** The definition does not capture a risk that relates only to persons who are the subject of a warrant, order or other lawful authority to access information. Put differently, a vulnerability that affects only the targets of a lawful authorization does not qualify as a systemic vulnerability.

As noted above, the government introduced much of the current systemic vulnerability language through amendments in June 2026, before the Bill was passed in the House of Commons on 18 June 2026 and after critique of the Bill’s previous framework. These amendments lowered the threshold for a systemic vulnerability risk from a “substantial risk” to a “credible risk”, added the reference to “recognized international technical standards”, and added the exception for risks confined to the targets of a lawful authorization. They also added an express decryption provision, now found in section 2(4) of the *SAIA* (House of Commons, Standing Committee on Public Safety and National Security, *Bill C-22, An Act respecting lawful access* ([Fifth Report](#)) (18 June 2026) at cl 41 (SECU Fifth Report); *Bill C-22*, first reading, *supra*). The decryption provision reads as follows:

[n]o 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 provides services, unless the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information. (*SAIA*, s 2(4))

In other words, an ESP cannot be compelled to decrypt information that its users have encrypted, unless the ESP itself supplied the encryption and holds the information necessary to decrypt it.

The *SAIA* gives force to its systemic vulnerability framework primarily through a series of compliance exemptions. A core provider need not comply with a provision of a regulation made under section 5(2) if compliance would have the effect of requiring it to introduce a systemic vulnerability into the service, or of preventing it from rectifying one (*SAIA*, s 5(5)). The same exemption applies to an ESP subject to a ministerial order under section 7(1) or a compliance order under section 24(1) (*SAIA*, ss 7(5), 24(2.1)). The *SAIA* reinforces this exemption in the provisions that require compliance with those orders (*SAIA*, ss 11, 25(1)), so the rule that a ministerial order prevails over an inconsistent regulation does not permit the government to bypass the safeguard (*SAIA*, s 12). This was a contention previously raised by critics of the Bill, who argued that its original enforcement provisions created a “structural contradiction” with the safeguard, and one that the June 2026 amendments rectified (see e.g., Michael Geist, [“Could Bill C-22 Make Canadians Less Safe? The Systemic Vulnerability Gap in Canada’s New Surveillance Law”](#) (8 April 2026), online (blog): Michael Geist; SECU Fifth Report, *supra* at cl 41).

1.1. Element 1: The Vulnerability Must Relate to the “Electronic Protections of an Electronic Service”

The scope of protection offered by the systemic vulnerability provision in C-22 turns, in part, on the definition of “electronic protection” (Geist, “Years of Uncertainty”, *supra*). This is because a “systemic vulnerability” under C-22 exists only with respect to vulnerabilities “in the electronic protections of an electronic service” (*SAIA*, s 2(1)). Section 2(1) defines “electronic protection” as “authentication, encryption and any other prescribed type of data protection” (*SAIA*, s 2(1)). The *SAIA* does not define “authentication” or “encryption”. Nor does it set out the criteria the government must apply in deciding which other types of data protection fall within “any other prescribed type of data protection” (*SAIA*, s 2(1), “electronic protection”), creating further uncertainty as to which protections the systemic vulnerability safeguard will ultimately cover.

These omissions are especially concerning because the *SAIA* empowers the Governor in Council to make regulations, “respecting the meaning of any term or expression for the purposes of this Act, other than the terms and expressions defined in it” (*SAIA*, s 47(1)(c)). Put simply, the government may later define “authentication” and “encryption” by regulation. It may also decide, by regulation, which other types of data protection qualify as “electronic protections”, since “prescribed” means “prescribed by the regulations” (*SAIA*, s 2(1), “prescribed”).

Nothing in the *SAIA* prevents the government from defining or prescribing these terms narrowly, and nothing requires it to do so in a manner that accords with accepted technical usage. A narrow definition would shrink the category of “electronic protections”, and with it, the scope of what constitutes a “systemic vulnerability” under the *SAIA*. We therefore cannot take for granted that the government will adopt an expansive or technically accepted definition of these terms. In fact, we should assume just the opposite, because the government has given itself the ability not to do so—and, more to the point, has refused to do so during the legislative process. The decryption provision (section 2(4) of the *SAIA*) offers little comfort in this regard. As we exemplify below, this provision only safeguards certain uses of encryption leaving others vulnerable to decryption.

To fully understand why the lack of specificity in the definition of “electronic protection” puts Canadians’ data at risk and why the decryption provision does not truly safeguard encryption, it is important to understand yet another concept: that of cryptography. The section that follows offers a brief overview of cryptography for non-technical readers. This divergence into cryptography is important at this stage of this post because our aim is to show that encryption is but one of several cryptographic protections, that encryption itself exists in several forms, and that the weakening of *any cryptographic protection*, not just encryption, can create a security vulnerability.

1.1.1 A Brief Primer on Cryptography

Cryptography is a set of mathematics-based tools and techniques that, when properly used, prevent eavesdropping, tampering, forgery, and suppression of messages during communications (data in motion) and when stored (data at rest). The Internet now connects billions of people. Its original design served closer to hundreds and contained no affordances for security. As people increasingly used the Internet to perform actions with real-world consequences (commerce, document signing, sending privileged communications, banking, even voting), security researchers built layers of security atop the protocols that underpinned the early Internet and still do so today. It is difficult to exaggerate the role cryptography plays in making the Internet suitable for any real-world application. Without cryptography, the ability of others to passively read, actively modify, or even impersonate users becomes a constant threat. The Internet is global in reach, so threat actors need not be physically proximate to cause mischief and disruptions. As we discussed in our [first post](#), even with cryptographic protections, these threats are becoming increasingly common.

1.1.1.1 Encryption

Encryption is a cryptographic technique that focuses on eavesdropping. For example: the sender Alice encrypts the actual message (the “plaintext”) to form a “ciphertext” and sends it to Bob, in the presence of an eavesdropper Eve. This ciphertext is indistinguishable from pure random noise (e.g., coin flips) unless one has the corresponding decryption key to decrypt the ciphertext and recover the plaintext. Encryption typically protects the contents of a communication from observation as it passes through the dozens of computers and networks involved when a user visits a website. Encryption is used when a user is browsing the web, formerly signalled with a “lock icon” (but now so ubiquitous only encryption’s absence is indicated with a broken-lock icon). Thus, encryption is used to secure communications between two parties.

The language of C-22 treats encryption as though it were a single method serving a single purpose. It is not. As this section demonstrates, encryption takes place in multiple contexts: end-to-end encryption between users, TLS encryption between a user and a website, which relies on the temporary session keys that protect individual connections, and with them past communications. Each offers different protections, yet it remains unclear whether “encryption” as defined under the *SAAIA* will extend to each of these uses. Worse, as discussed below, not all of them are protected by the decryption provision in section 2(4).

1.1.1.2 End-to-end Encryption

“End-to-end encryption” (E2EE) is the technique under which only the two communicating parties can decrypt their communications; as such, they are secure against active attacks such as message addition, deletion, and modification. Signal is an example of a messaging service that uses E2EE. Signal is designed so that end users *do not need* to trust the infrastructure that simply moves messages between devices. When Alice sends a message to a friend Bob, she does so first by sending it through Signal’s servers; after all, Bob may be offline. Despite holding the data, Signal is unable to decrypt it or understand its contents as only Bob is able to decrypt it when he finally receives it, because only Bob has the key. It is thus encrypted end (Alice) to end (Bob). The same notion of E2EE can be used for email delivery, where a service that stores mail, such as Proton Mail, only stores encrypted data Proton Mail itself cannot recover, only the user can.

Section 2(4) of the *SAAILA* protects this use of encryption. It provides that no obligation under the *Act* is to be construed as compelling an ESP to decrypt information encrypted by its users, unless the ESP itself provided the encryption and possesses the information necessary to decrypt it (*SAAILA*, s 2(4)). In a properly implemented E2EE system, the ESP never holds the keys needed to decrypt its users’ communications. Therefore, the *SAAILA* cannot compel it to decrypt them. (Note: there is one concern about what is precisely meant by “provided the encryption”, which we revisit when discussing compromised software updates in Part 0 of this post).

E2EE as a concept is inconsistent with any form of lawful access other than law enforcement access at one of the two devices that are the actual endpoints of the communication. Any key escrow or systematic, deliberate undermining of E2EE for all Canadians necessarily means that a third party to the communications, such as the service provider, must store and access that information, or law enforcement is surreptitiously added as a “ghost user” to some or all E2EE conversations. Many such service providers are foreign entities. Canadians’ data would therefore become readily available to foreign governments under their own distinct access provisions, which may have fewer safeguards than Canadians expect and deserve.

1.1.1.3 Encryption Between a User and a Website

For most Internet users, encryption is most frequently used between their browser or device and the Internet sites they visit. The protocol used is called Transport Layer Security (TLS). TLS is said to provide E2EE between the user and the website. When multiple users communicate with each other mediated by a website, for example, when Alice visits Bob’s profile on a website and sends Bob a “direct” message (which is actually through the website), Alice and Bob do not have E2EE with regard to that message. Instead, each has a separate TLS connection with the website, which decrypts Alice’s message on arrival and re-encrypts it to send to Bob. The webserver thus has one E2EE-key (or session key) for Alice and another for Bob and can easily be said to be providing encryption, albeit in a different form than what Signal provides in the example above, because in this case, the webserver holds the decryption key.

This difference has the consequence of removing this use of encryption from the protection offered by section 2(4), which expressly excludes circumstances where the ESP provided the encryption and holds the key. As a result, as currently written, nothing in section 2(4) precludes the

government from requiring the website to decrypt Alice and Bob's messages (*SAAILA*, s 2(4)). The specific inclusion of this exception suggests that Parliament contemplated access to precisely this sort of information. Any protection for TLS must therefore come from the "systemic vulnerability" exemption, which is itself fraught with uncertainty, notwithstanding the fundamental role TLS plays in securing the Internet.

An important aspect of TLS is the use of "session keys": these are ephemeral and so when the connection between the user and the website ends, the browser deletes the session key, and in practice so too should the server. Session keys may only exist for minutes or seconds. For example, Signal updates session keys every time there is a back-and-forth round of communication. This is intentional, because it provides that anyone who records encrypted traffic now and then later compromises a user's device cannot retroactively decrypt previously terminated communications (this is called forward security). Of course, if you keep all your messages on your phone someone who steals your phone can read them, but the encryption keys used to secure the messages as they travelled the Internet are long gone.

Compelling web servers to store, or even delay deleting, these session keys would undoubtedly create vulnerabilities in TLS. It would defeat forward security, allowing anyone who obtains the stored keys, whether by compromising the server or otherwise, to decrypt previously recorded traffic retroactively. Once again, the decryption provision in section 2(4) of the *SAAILA* would offer no protection against such a requirement, because the website both provides the encryption and holds the session key. As a result, nothing in section 2(4) would prevent the government from compelling the website to retain those keys and to use them to decrypt its users' communications (*SAAILA*, s 2(4)). Similarly, session keys are negotiated using variants of a key negotiation protocol called Diffie-Hellman. This protocol requires random key-negotiation parameters from both parties, and nothing in section 2(4) would prevent a server from being compelled to provide random-looking but predictable key-negotiation parameters for some or all users to simplify its compliance under the *Act*. Here too, any protection must come from the ill-defined "systemic vulnerability" exemption. This is particularly problematic because a session key does not itself reveal anything; it does so only when combined with traffic recorded by other means, which, as we discuss in Part 1.2, raises the question of whether the risk threshold in the "systemic vulnerability" definition will be met (*SAAILA*, s 2(1)).

Combined with recorded traffic, retained session keys would expose not merely which websites a user visited, but the full content of those visits, including the pages viewed, messages sent, searches made and passwords entered. Nor would the exclusions in section 5(4) clearly prevent such a requirement. As we discussed in our [second post](#), the *SAAILA* permits regulations requiring core providers to retain metadata for up to six months (*SAAILA*, s 5(2)(d)). Section 5(4) limits that power: a metadata retention regulation may not require a provider to retain information that "would reveal" the content of communications, a person's "web browsing history" or their "social media activities" (*SAAILA*, s 5(4)). These exclusions, however, apply only to regulations made under section 5(2)(d). They do not restrict the government's other regulation-making powers, including its power to require core providers to develop "operational and technical capabilities" (*SAAILA*, s 5(2)(a)). A requirement to retain session keys could therefore be framed as a technical capability rather than as metadata retention, placing it outside the section 5(4) exclusion altogether. The result

is that the *SAAILA* could permit, indirectly, what section 5(4) purports to exclude: the retention of information capable of revealing the content of communications and a person's browsing history.

By excluding cases in which “the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information”, section 2(4) leaves open the possibility that the government may require ESPs to weaken or decrypt certain forms of encryption, thereby undermining data security for all Canadians, and, in the case of TLS and session keys, permitting the retention of information capable of revealing the very content and browsing history that the *Act* elsewhere excludes from its retention requirements (*SAAILA*, ss 2(4), 5(4)). Parliament should consider removing this exception, particularly since the state has at its disposal existing tools to compel the production of this type of information under the *Criminal Code*, including production orders, authorizations to intercept private communications, and assistance orders requiring a person to help give effect to those authorizations (*Criminal Code*, [RSC 1985, c C-46](#), ss 186, 487.014, 487.02; *SAAILA*, s 2(2)):

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

Since the Bill's introduction, much of the commentary has focused on the risk that the government will use C-22 to weaken encryption. This attention is not undeserved. Indeed, encryption is one of the most important privacy-enhancing technologies of the modern era. That said, the focus on encryption is far too narrow. Encryption is only one part of the broader field of cryptography. Accordingly, we undertake a high-level survey of other cryptographic methods below.

1.1.1.4 Message Authentication Codes and Digital Signatures

Concerns about weakening encryption dominate the debate over C-22, but cryptography plays other critical roles beyond confidentiality, namely integrity and authenticity. Cryptographic message authentication codes (MACs) and digital signatures are used to protect against message and data tampering (including creating new messages or deleting parts of messages), and can be used to authenticate the author of messages. These tools can also be used to ensure that no messages were omitted by numbering each message and authenticating that numbering. Message integrity with MACs relies on both Alice and Bob sharing a secret key that they use to both generate and validate the MACs.

Digital signatures are different, resembling signatures in the physical world where only one person can produce the characteristic signature but everyone else can verify it. In this case, a signer creates two connected keys, a public one and a private one, and can produce signatures with the private key that can be verified with the public key. The only requirement for someone wanting to verify a signature on a message is that they have the authentic public key for the author. Unlike a MAC key, which both parties must keep secret, the signer can, and should, share a public key with everyone who needs to verify a signature.

Weakening these protections would not, on its own, reveal the content of communications. It would do something potentially more dangerous: allow messages to be altered, forged or silently deleted. In particular, ESPs could be forced to provide software updates that cause users' software to exhibit spyware-like qualities, reading and intercepting communications without ever technically breaking encryption. While signing such malware is fraught given that it may easily end up being installed on the computers of non-targets, such as in the case of [Stuxnet](#), C-22 does not do anything to address this obvious vulnerability. Because compelling an ESP to sign a malicious update does not require it to decrypt anything, the decryption provision in section 2(4) offers no protection. Any protection must instead come from the "systemic vulnerability" exemption, and therefore depends on whether "authentication", which the *SAAILA* leaves undefined, is read to include digital signatures (*SAAILA*, s 2(1), "electronic protection").

1.1.1.5 Third-Party Scripts

Moreover, the behaviour of every webpage is dynamically controlled through a programming language called JavaScript. Websites indicate the JavaScript files they need to operate, and oftentimes these are retrieved from different websites than the one being visited, or by "content distribution networks" (CDNs). Were these CDNs designated as ESPs, they could be compelled to distribute JavaScript files that can report what the user sees and does on the resulting website, again without doing anything to break encryption. There are cryptographic measures that can be used to validate that the script is authentic, but the use of them is at the discretion of the website itself, which can be compelled to remove the protections. Once again, because neither requirement involves decryption, section 2(4) offers no protection. Nor is it clear that the systemic vulnerability exemption would apply. The measures that validate a script check its integrity, and the *SAAILA* does not say whether such measures qualify as "authentication", "encryption" or "any other prescribed type of data protection" within the definition of "electronic protection" (*SAAILA*, s 2(1)). If they do not, a requirement to remove them falls outside the safeguard altogether.

1.1.1.6 Back Doors

Security experts call an intentional defect within an otherwise secure system, created for any reason including lawful access, a "back door". Back doors cannot coexist with security, because they make the security of every Internet user rely on the perpetual secrecy of the small amount of information required to exploit the back door. If the government held the general capability to break encrypted communication, with the promise to use it only under appropriate circumstances, it would do so by holding some particular information (in some form) that lets it open and enter the back door. This means that any entity with that same information could do the same and so the security of all Canadians rests on the unlikely assumption that the information will never be known by a bad actor or a foreign intelligence service. Worse still, a threat actor who collects network traffic today can decrypt it years later, once it understands how the back door works.

The foregoing is necessarily a brief overview of a complex field. Indeed, a comprehensive explanation of cryptography is beyond the scope of this post. However, we hope that the above is sufficient to convey that the weakening of any cryptographic protection, not just encryption (in its various forms), can create a vulnerability, and yet not every such vulnerability is guaranteed to fall within the definition of "systemic vulnerability", nor to be precluded by the decryption provision

in section 2(4). We therefore conclude that systemic vulnerability safeguards should capture all base cryptographic techniques by simply referring to cryptography generally instead of discrete methods.

1.1.2 Cryptography is Not Mentioned in Reference to “Electronic Protection” or in the SAAIA At All

The *SAAIA* makes no mention of the term “cryptography” whatsoever. Read generously, one might suggest that the phrase “any other prescribed type of data protection” in the definition of “electronic protection” might capture standard cryptographic techniques not otherwise explicitly named (*SAAIA*, s 2(1)). We suggest it would be unwise to rely on that reading. We cannot assume that “electronic protection” will be read to include all standard cryptographic techniques. The inclusion of the term “prescribed” further undermines the suggestion that the term “electronic protection” will be construed broadly. Instead, it indicates that the government will decide, by regulation, which standard cryptographic techniques fall within the scope of an “electronic protection” (*SAAIA*, s 2(1), “prescribed”).

The lack of specificity in the definition of “electronic protection”, coupled with the government’s discretion to define its terms narrowly at some future date rather than in the legislation itself, leaves open the possibility that the systemic vulnerability safeguard in the *SAAIA* is far narrower than it appears. Any cryptographic protection that falls outside the definition falls outside the framework as well. If the government were to require an ESP to weaken such a protection, the ESP could not rely on the exemptions created in sections 5(5), 7(5) and 24(2.1) to refuse to comply, and the resulting vulnerability would expose the data of every Canadian who uses that service.

1.1.3 Proposed Amendments

We propose that Parliament consider amending section 2(1) of the *SAAIA* in the following respects. First, it should replace the current definition of “electronic protection” with a definition grounded in what a protection does, covering cryptographic and other technical protections. As discussed above, encryption and authentication are only two of the protections that cryptography provides. Removing the word “prescribed” from the definition in section 2(1) would also ensure that the government cannot shape the scope of the safeguard by regulation. Although this definition is broad, a weakening of an electronic protection would qualify as a systemic vulnerability only if it creates a credible risk of unauthorized access to secure information, so the safeguard would not extend to every technical change an ESP might be required to make. Second, Parliament should define “authentication”, “cryptography”, and “encryption” in the *Act* itself to assuage concerns that the government will use its discretion under section 47(1)(c) to construe these terms narrowly at a later date. Third, the definition of “systemic vulnerability” should make clear that it includes any weakening, undermining or reduction in the effectiveness of an electronic protection that creates a credible risk of unauthorized access to secure information.

These proposed amendments are listed below.

1.1.3.1 Amended Definition: “Electronic Protection” (s 2(1))

electronic protection means ~~authentication, encryption and any other prescribed type of data protection~~ any measure that uses cryptography or other technical means to protect the confidentiality, integrity or authenticity of information or of an electronic service, including authentication and encryption.

1.1.3.2 New Definitions (s 2(1))

authentication means any process that uses cryptography or other technical means to verify the identity of a person or device, or the origin and integrity of data, including through digital signatures and message authentication codes.

cryptography means the use of mathematical techniques to protect information against unauthorized access, alteration, forgery or suppression, including through encryption, digital signatures and message authentication codes.

encryption means the process by which an encryption key is used to convert plaintext into ciphertext for the purpose of preventing the plaintext from being computed from the ciphertext without knowledge of the corresponding decryption key.

1.1.3.3 Addition to the Definition of “Systemic Vulnerability” (s 2(1))

...For greater certainty, a systemic vulnerability includes any weakening, undermining or reduction in the effectiveness of an electronic protection that creates such a risk.

1.2 Element 2: The Vulnerability Must Create a “Credible Risk” Based on “Recognized International Technical Standards”

The second element of the definition of “systemic vulnerability” concerns the degree of risk a vulnerability must create. A vulnerability qualifies as “systemic” only if it creates “a credible risk, based on recognized international technical standards, that secure information could be accessed by a person who does not have any right or authority to do so” (*SAAILA*, s 2(1)). This threshold determines how serious a risk must be before an ESP may refuse to comply with a regulation or order (*SAAILA*, ss 5(5), 7(5), 24(2.1)).

The June 2026 amendments lowered the threshold for a risk to come within the definition of “systemic vulnerability”, from a “substantial” risk to a “credible” one. In our view, this amendment represents a positive step toward safeguarding Canadians’ data. However, the same amendments also tied that risk to “recognized international technical standards”, which the *SAAILA* leaves undefined and the government may therefore define later by regulation (*SAAILA*, s 47(1)(c)). This definition, in turn, will affect which risks qualify as “credible” and fall within the definition of “systemic vulnerability”.

Indeed, the phrase “recognized international technical standards” is misleading in and of itself. It suggests that an international consensus exists on the technical standards, metrics and

methodologies for assessing whether a vulnerability creates a credible risk. It also suggests that one or more international bodies set and oversee such standards. In practice, the landscape is fragmented. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly publish information security standards, such as the ISO/IEC 27000 series; the Internet Engineering Task Force (IETF) publishes protocol and security standards through its Requests for Comments (RFCs); MITRE, a US-based not-for-profit, maintains the Common Vulnerabilities and Exposures (CVE) catalogue of known vulnerabilities; and the Open Worldwide Application Security Project (OWASP) publishes widely used, but informal, security guidance. Each is influential, yet none is a governing body or Treaty, each is different, and none was designed to determine when a lawful access requirement creates a systemic vulnerability in an otherwise secure system.

The *SAIA* does not say which of these sources, if any, counts as a “recognized international technical standard”, nor what happens when they conflict. In other words, although many organizations participate in this sphere, no single authority determines when a risk is credible. The requirement that the risk be credible “based on recognized international technical standards” is therefore at best a meaningless platitude, and at worst a placeholder for a narrower definition to come. If the government has a particular set of standards in mind, it should identify them; without so doing, there are no standards playing a role here.

1.2.1 Proposed Amendment

Parliament should amend the definition of “systemic vulnerability” in section 2(1) to remove the words “based on recognized international technical standards”, so that the safeguard turns on whether a vulnerability creates a credible risk of unauthorized access, rather than on an imaginary unified international benchmark.

systemic vulnerability means a vulnerability in the electronic protections of an electronic service that creates a credible risk, ~~based on recognized international technical standards,~~ that secure information could be accessed by a person who does not have any right or authority to do so...

1.3 Exception: Risks Confined to the Targets of a Lawful Authorization

The final component of the definition of “systemic vulnerability” is an exclusion. A risk does not qualify as a systemic vulnerability if it “relates only to information related to persons with respect to whom a warrant, order or other authority to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act* — or any similar authority conferred under another Act of Parliament — applies” (*SAIA*, s 2(1)). In other words, if a weakness puts at risk only the information of people already subject to a lawful authorization, such as the target of a warrant, it falls outside of the definition of “systemic vulnerability”.

On its face, the exclusion reflects a sensible distinction: lawful access is meant to reach the targets of an authorization, and the safeguard is meant to protect everyone else. The difficulty with this exception is that it is hard to conceive that a vulnerability for one will not be a vulnerability for all. In effect, the exception permits the government to require what security experts call a “back

door” (an intentional weakness built into an otherwise secure system for the purpose of lawful access) provided the resulting risk can be characterized as confined to the targets of a lawful authorization. As Robert Diab observes, if a company is asked to create a risk “that police acting with a warrant could exploit, then it would seem to be one that hackers could also exploit” (Robert Diab, [“Parliament Has Amended Bill C-22, But Has It Addressed the Biggest Privacy Concerns?”](#) (19 June 2026), online (blog): *Robert Diab*). The efficacy of the exclusion turns on the assumption that ESPs will be able to confine the vulnerability to the information of a person subject to a lawful authorization. This assumption is simply not based in technological reality. A capability built to reach one target usually must exist across the whole system, thus having the potential to compromise the whole system.

The exclusion also assumes that a capability built for a lawful target will remain in lawful hands. As with any back door, anyone who learns how to open it can use it. A vulnerability that “relates only to” the target of a warrant on the day the government uses it does not stay confined to that target if the capability is lost, stolen, or reverse-engineered. This risk can be avoided entirely only by not building the back door in the first place.

Software updates offer a concrete example of both problems and illustrate the crucial role digital signatures play. Computers, including routers and mobile phones, routinely download software updates “over the air” and install them at the manufacturer’s request. Some operating systems cease functioning if a user does not install these updates; others install them without any user involvement whatsoever. The digital signature on the code underpins the security of this system: it confirms that the code comes from the manufacturer and that no other party has modified it, and so that it is safe to install. Suppose the government required a provider to deliver a modified software update to a single device named in a warrant, for example to install forensic spyware. The update may reach only that device, but the provider can deliver it only through an update channel that could reach any device on its service. Other people’s devices may end up accepting such updates, and non-government sources may end up supplying them.

The government could nevertheless characterize the use of the capability as targeted, and so excluded from the definition of “systemic vulnerability”, even though the capability itself creates a risk for every user. The *SAAILA* does not say whether the exclusion looks to the targeted use or to the system-wide capability that makes it possible. Put differently, the *Act* leaves open whether a vulnerability that exists for everyone, but is exploited against only one person, “relates only to” that person. There is simply no good reason for such ambiguity.

Further uncertainty arises because the *SAAILA* sets out no criteria or dedicated procedure for deciding whether a risk is confined to the target of a lawful authorization. Nor does it define what it means for a risk to “relate only to” such a target, leaving the Governor in Council free, once again, to give that expression meaning by regulation (*SAAILA*, s 47(1)(c)). As we will discuss below, ESPs will in practice bear the burden of demonstrating that a regulation or order will create a vulnerability that is systemic and not confined to the target of the lawful authorization. Part 2 examines the allocation of this burden and its consequences for ESPs, particularly those with limited resources.

1.3.1 Proposed Amendments

Parliament should amend the definition of “systemic vulnerability” to remove the exception for risks that relate only to the targets of a lawful authorization, which rests on the faulty and technically unrealistic assumption that a vulnerability created for lawful access can be confined to its intended target.

systemic vulnerability means...that secure information could be accessed by a person who does not have any right or authority to do so, ~~other than a risk that relates only to information related to persons with respect to whom a warrant, order or other authority to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act* or any similar authority conferred under another Act of Parliament~~ applies.

2. Structural Limitations of the Systemic Vulnerability Safeguard and the Consequences

The definitional gaps discussed above concern what counts as a systemic vulnerability. Even where a requirement clearly meets that definition, however, the safeguard’s protection is limited by its structure. As drafted, the *SAAILA* does not preclude the government from making future regulations or orders that would introduce a “systemic vulnerability” or vulnerability for that matter. Instead, it relieves ESPs of the obligation to comply with them if such regulations are made (*SAAILA*, ss 5(5), 7(5), 24(2.1)). The government may therefore make a regulation or order regardless of whether it creates a systemic vulnerability, leaving it to the ESP to object after the fact.

2.1 Who Bears the Burden? The Practical Consequences for ESPs

In practice, the *SAAILA* will require designated ESPs to facilitate the state’s lawful access to Canadians’ data both by retaining that data (as we discussed in our [second post](#)) and by enabling the state’s later requests to access data. At the same time, ESPs, which must also provide “all reasonable assistance” with the testing of lawful access tools (*SAAILA*, s 13(1)), will bear the primary burden of identifying, rectifying, and in cases where a solution cannot be engineered, demonstrating that the government’s demands would introduce “systemic vulnerabilities” into their systems or prevent the ESP from rectifying a systemic vulnerability (*SAAILA*, ss 5(5), 7(5)).

Recall from our [first post](#) that the definition of an ESP is unreasonably broad and essentially amounts to an inventory of the digital world. The *SAAILA* is likely to impose an extraordinary burden on ESPs; but what that burden will involve in practice remains unclear. The *SAAILA* contemplates regulations respecting both the “development, implementation, assessment, testing and maintenance of operational and technical capabilities” and the installation and operation of “any device, equipment or other thing ... that may enable an authorized person to access information” (*SAAILA*, s 5(2)(a), (b)). It does not say whether the government will supply the tools that ESPs must deploy, or whether ESPs must build their own to specifications the government has yet to set. Each model raises different questions: who maintains and updates the capability, who answers for a vulnerability it introduces, and whether an ESP can inspect code it did not write. As Professor Michael Geist observes, Parliament is being asked to approve the framework

“without knowing who will be covered, what they will be required to build” (Geist, “Years of Uncertainty”, *supra*).

The burden imposed by the *SAAILA* will be especially acute for not-for-profit and hobbyist developers whose software happens to be widely deployed in network communications. Although the *Act* requires the government to consider compliance costs, both when it makes regulations for core providers and when the Minister makes an order (*SAAILA*, ss 5(3)(c), 7(3)(c)), it provides for compensation only in the case of ministerial orders, and then only at the Minister’s discretion and in an amount “the Minister considers appropriate” (*SAAILA*, s 7(4); see also s 47(1)(a) (fees for assistance with lawful access requests)). Core providers subject to regulations have no comparable compensation mechanism.

At this point, we would be remiss not to address the role of volunteer and open-source developers. Much of the Internet’s security infrastructure is built and maintained by developers who work on open-source projects without any expectation of profit. As the OpenSSL example below illustrates, a small team of volunteers can maintain software on which millions of people depend. Many of these developers may fall within the *SAAILA*’s broad definition of an “electronic service provider” (*SAAILA*, s 2(1)). It would be a mistake to assume that the lack of a profit-motive in their work means either that their projects are unimportant, or that they are too insignificant to attract the state’s interest in the data that flows through them. The security of the Internet depends on many of these projects, and that same centrality makes them attractive targets for lawful access.

Requiring such developers to build lawful access capabilities raises a further difficulty. Software is difficult to write correctly, and secure software is more difficult still. Even well-resourced teams routinely ship vulnerabilities that go undetected for years. Deliberately weakening a system’s security without breaking it is harder again, because the developer must introduce a controlled weakness while preserving every other protection the system provides. In other words, a developer asked to build access for one party risks creating an unintended vulnerability that any party could exploit and may not discover the error until it has been exploited. It is unreasonable to expect volunteer developers, or indeed most developers, to design and implement what amounts to sophisticated surveillance software without introducing a systemic risk to all of its users.

OpenSSL is illustrative of the operating constraints under which many smaller ESPs function and the degree to which open-source software developed by hobbyists is ubiquitously relied upon. Its software library secures connections between web browsers and servers across much of the Internet, yet in 2014, when the “Heartbleed” vulnerability came to light, the project employed “just a single full-time developer” and had received “a grand total of \$2,000 in donations” the previous year (Robert Lemos, “[Where’s the Next Heartbleed Bug Lurking?](#)” *MIT Technology Review* (29 April 2014)). Canadians felt the consequences directly. Attackers exploited Heartbleed to steal the social insurance numbers of approximately 900 taxpayers from the Canada Revenue Agency (CRA) over a six-hour period (Wojtek Gwiazda, “[900 government ID numbers \(SIN\) stolen from Canada Revenue Agency data bank](#)” *Radio Canada International* (14 April 2014)). The CRA shut down its website in response and did not restore public access for about five days (Andre Mayer, “[Heartbleed bug shows governments slow to react](#)” *CBC News* (15 April 2014)).

It is difficult to overstate the importance of a number of small, under-resourced projects already maintaining some of the most critical security infrastructure that Canadians rely on. Adding *SAAILA* compliance obligations to their volunteer workload risks diverting scarce resources from the very security maintenance that protects Canadians' data, or worse, risks driving these secure services out of Canada altogether.

2.2 Procedural Safeguards and Who Must Invoke Them

The *SAAILA* does contain some procedural safeguards, though none prevent the government from imposing a requirement that would create a “systemic vulnerability” or any other vulnerability. In making regulations or orders, the Governor in Council and the Minister must take into account “the potential impact... on privacy protection and cybersecurity” (*SAAILA*, ss 5(3)(e), 7(3)(e)). Before making a ministerial order, the Minister must give the affected provider an opportunity to make representations (*SAAILA*, s 8). No order is valid unless the Intelligence Commissioner approves it (*SAAILA*, s 7(2)). An ESP may also seek judicial review in the Federal Court, after giving the Minister at least 15 days' written notice (*SAAILA*, s 17).

These safeguards, however, depend on the ESP's capacity to use them. None requires the government to obtain independent security expertise, and an obligation to “take into account” privacy and cybersecurity impacts is a weak constraint, if it is a constraint at all. In practice, an ESP must identify the vulnerability, establish that compliance would introduce it, and press that position through representations or litigation. A volunteer-run project may lack the legal and technical capacity to do so. Worse still, the *SAAILA* prohibits an ESP from disclosing the contents of a ministerial order or even the fact that it is subject to one, so the project cannot readily turn to the public, the press or the wider security community for support (*SAAILA*, ss 14(a), (c), 15). Meanwhile, non-compliance exposes the provider to administrative monetary penalties of up to \$50,000 for an individual and \$250,000 for any other person, with each day of a continuing violation counted as a separate violation (*SAAILA*, s 29(2), (3)). Realistically, such a group may have three options: comply with an obligation it believes weakens its users' security, contest the obligation without the means to do so, or withdraw its services from Canada.

The Privacy Commissioner raised the underlying weakness before the House of Commons Standing Committee on Public Safety and National Security during its study of the Bill, observing that the exemptions as drafted would not strictly prohibit the making of regulations or orders that result in a systemic vulnerability. The Commissioner recommended that sections 5(5) and 7(5) instead provide that regulations and orders “must not have the effect of” requiring an ESP to introduce, or preventing it from rectifying, a systemic vulnerability (Office of the Privacy Commissioner of Canada, “[Submission to the Standing Committee on Public Safety and National Security on its study of Bill C-22, An Act Respecting Lawful Access](#)” (21 May 2026), Recommendation 6). The committee did not adopt that recommendation. In other words, the safeguard operates as a defence that an ESP must invoke to justify non-compliance, rather than as a limit on the government's power to impose the requirement in the first place.

2.2.1 Proposed Amendments

Parliament should adopt the Privacy Commissioner’s Recommendation 6 and limit the power to make regulations and orders, rather than relying solely on an exemption from compliance. A regulation or order that “must not have the effect of” introducing a “systemic vulnerability” would be invalid to the extent that it did so. The government would therefore have to address the question before acting, and a court on judicial review could set aside a regulation or order that created a “systemic vulnerability”. This amendment would not remove the practical burden on ESPs, which would still need to identify the vulnerability and challenge the requirement. It would, however, place an obligation not to create “systemic vulnerabilities” on the government, where it belongs. Our only variation from the Privacy Commissioner’s recommendation is to add a new subsection to sections 5 and 7 of the *SAAILA*, rather than amend sections 5(5) and 7(5).

Limit on regulations

5(5.1) A regulation made under subsection (2) must not have the effect of requiring a core provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

Limit on orders

7(5.1) An order made under subsection (1) must not have the effect of requiring the electronic service provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

3. Obligation to Assist: Section 13

One provision remains outside the systemic vulnerability framework entirely. Section 13(1) of the *SAAILA* requires an ESP, on the Minister’s request, to “provide all reasonable assistance to a person or class of persons specified in the request to permit the assessment or testing of any device, equipment or other thing that may enable an authorized person to access information” (*SAAILA*, s 13(1)). The only limit is that the assessment or testing “must not have the effect of granting access to personal information” (*SAAILA*, s 13(4)). Unlike the duties to comply with regulations, ministerial orders and compliance orders (*SAAILA*, ss 5(5), 7(5), 11, 24(2.1), 25(1)), the obligation to assist is not made subject to any systemic vulnerability exemption. This omission is inconsistent with the rest of the framework, and a violation of section 13(1) carries with it administrative monetary penalties of up to \$50,000 for an individual and \$250,000 for any other person (*SAAILA*, s 29(1)(a), (2)).

3.1.1 Proposed Amendments

Parliament should amend section 13 to provide that an ESP is not required to provide assistance that would have the effect of introducing a systemic vulnerability into its services, or of preventing it from rectifying one. Because the application of section 13 is not confined to ESPs that are core providers or subject to a ministerial order, we suggest an amendment as follows:

Obligation to assist

13 (1) Subject to subsection (1.1), on request made by the Minister, an electronic service

provider must provide all reasonable assistance to a person or class of persons specified in the request to permit the assessment or testing of any device, equipment or other thing that may enable an authorized person to access information.

Systemic vulnerability

(1.1) An electronic service provider is not required to provide assistance under subsection (1) if providing that assistance would have the effect of requiring the provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

That said, it is unclear why section 13 is not confined to core providers or to ESPs subject to a ministerial order, particularly given the breadth of the definition of an ESP (*SAIA*, s 2(1)). David Fraser made the same point shortly after the Bill's introduction (David TS Fraser, "[The Deeply Problematic Part 2 of Bill C-22: The Supporting Authorized Access to Information Act](#)" (20 April 2026), online (blog): *Canadian Privacy Law Blog* (discussing what was then s 14)). As drafted, the obligation extends to any ESP the Minister chooses to name in a request, and the only qualifications are that the assistance be "reasonable" and that the testing not grant access to personal information (*SAIA*, ss 13(1), (4)). In other words, section 13 would allow the government to conscript virtually any ESP into testing its lawful access tools. As we noted in our [first post](#), the definition of an ESP is "so sweeping and overbroad" that it captures "nearly every business operating in Canada". Parliament should also narrow section 13 so that it applies only to core providers and to ESPs subject to a ministerial order. Such an amendment may read as follows:

Obligation to assist

13 (1) Subject to subsection (1.1), on request made by the Minister, ~~an electronic service provider~~ a core provider, or an electronic service provider that is subject to an order made under subsection 7(1), must provide all reasonable assistance to a person or class of persons specified in the request to permit the assessment or testing of any device, equipment or other thing that may enable an authorized person to access information.

Systemic vulnerability

(1.1) An electronic service provider is not required to provide assistance under subsection (1) if providing that assistance would have the effect of requiring the provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

Because the Minister may make an order with respect to any ESP, "whether or not the provider is a core provider" (*SAIA*, s 7(1)), this amendment would not prevent the government from seeking assistance from a particular ESP. It would, however, require the government to proceed through the order process, which entitles the ESP to make representations, requires the approval of the Intelligence Commissioner, requires the Minister to consider compliance costs and permits compensation, and engages the systemic vulnerability exemption (*SAIA*, ss 7(2)–(5), 8).

4. Summary of Proposed Amendments

For ease of reference, we set out below each of the amendments to the *SAAILA* recommended in this post. As noted above, we offer this language to illustrate how Parliament might address the concerns we identify, and not as text to be adopted wholesale. Proposed additions are underlined and proposed deletions are struck through.

4.1 Amended Definition of “Electronic Protection” (s 2(1))

Parliament should replace the current definition with one grounded in what a protection does, rather than a list of named techniques, and remove the word “prescribed” so that the government cannot narrow the scope of the safeguard by regulation.

electronic protection means ~~authentication, encryption and any other prescribed type of data protection~~ any measure that uses cryptography or other technical means to protect the confidentiality, integrity or authenticity of information or of an electronic service, including authentication and encryption.

4.2 New Definitions of “Authentication”, “Cryptography” and “Encryption” (s 2(1))

Parliament should define these terms in the *Act* itself, so that their meaning falls outside the Governor in Council’s power to define undefined terms by regulation (*SAAILA*, s 47(1)(c)).

authentication means any process that uses cryptography or other technical means to verify the identity of a person or device, or the origin and integrity of data, including through digital signatures and message authentication codes.

cryptography means the use of mathematical techniques to protect information against unauthorized access, alteration, forgery or suppression, including through encryption, digital signatures and message authentication codes.

encryption means the process by which an encryption key is used to convert plaintext into ciphertext for the purpose of preventing the plaintext from being computed from the ciphertext without knowledge of the corresponding decryption key.

4.3 Amended Definition of “Systemic Vulnerability” (s 2(1))

Parliament should remove the reference to “recognized international technical standards” and the exception for risks confined to the targets of a lawful authorization, and clarify that the definition captures any weakening, undermining or reduction in the effectiveness of an electronic protection that creates a credible risk of unauthorized access to secure information.

systemic vulnerability means a vulnerability in the electronic protections of an electronic service that creates a credible risk, ~~based on recognized international technical standards,~~ that secure information could be accessed by a person who does not have any right or authority to do so, ~~other than a risk that relates only to information related to~~

~~persons with respect to whom a warrant, order or other authority to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act* — or any similar authority conferred under another Act of Parliament — applies. For greater certainty, a systemic vulnerability includes any weakening, undermining or reduction in the effectiveness of an electronic protection, that creates such a risk.~~

As amended, the definition would read:

systemic vulnerability means a vulnerability in the electronic protections of an electronic service that creates a credible risk that secure information could be accessed by a person who does not have any right or authority to do so. For greater certainty, a systemic vulnerability includes any weakening, undermining or reduction in the effectiveness of an electronic protection that creates such a risk.

4.4 Amended Decryption Provision (s 2(4))

Parliament should remove the exception for encryption that an ESP provides and for which it holds the information necessary to decrypt, so that the decryption provision protects all forms of encryption.

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

As amended, the provision would read:

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 provides services.

4.5 Limits on Regulations and Orders (ss 5(5.1), 7(5.1))

Parliament should adopt the Privacy Commissioner's Recommendation 6 by adding new subsections to sections 5 and 7 providing that regulations and orders must not have the effect of introducing, or preventing the rectification of, a systemic vulnerability, while retaining the existing exemptions in sections 5(5) and 7(5).

Limit on regulations

5(5.1) A regulation made under subsection (2) must not have the effect of requiring a core provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

Limit on orders

7(5.1) An order made under subsection (1) must not have the effect of requiring the electronic service provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

4.6 Amended Obligation to Assist Provision (s 13)

Parliament should confine the obligation to assist to core providers and ESPs subject to a ministerial order, and add a systemic vulnerability exemption consistent with those in sections 5(5), 7(5) and 24(2.1).

Obligation to assist

13 (1) Subject to subsection (1.1), on request made by the Minister, ~~an electronic service provider~~ a core provider, or an electronic service provider that is subject to an order made under subsection 7(1), must provide all reasonable assistance to a person or class of persons specified in the request to permit the assessment or testing of any device, equipment or other thing that may enable an authorized person to access information.

Systemic vulnerability

(1.1) An electronic service provider is not required to provide assistance under subsection (1) if providing that assistance would have the effect of requiring the provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

As amended, the provisions would read:

Obligation to assist

13 (1) Subject to subsection (1.1), on request made by the Minister, a core provider, or an electronic service provider that is subject to an order made under subsection 7(1), must provide all reasonable assistance to a person or class of persons specified in the request to permit the assessment or testing of any device, equipment or other thing that may enable an authorized person to access information.

Systemic vulnerability

(1.1) An electronic service provider is not required to provide assistance under subsection (1) if providing that assistance would have the effect of requiring the provider to introduce a systemic vulnerability related to an electronic service or of preventing the provider from rectifying such a vulnerability.

This post may be cited as: Alexandra Lyn, Joel Reardon & Michael Nesbitt, “Decrypting Bill C-22, Part III: Backdoors by Another Name: The Limits of C-22’s Systemic Vulnerability Safeguard” (26 October 2026), online: ABlawg, http://ablawg.ca/wp-content/uploads/2026/10/Blog_AL_BillC22_Part3.pdf

To subscribe to ABlawg by email or RSS feed, please go to <http://ablawg.ca>

Follow us on Twitter [@ABlawg](#)

