

Building the *Cybersecure* Canada We Want in 2050

QSC Recommendations regarding the Importance of Cybersecure Infrastructure:

- 1. The National Infrastructure Assessment should include a comprehensive approach to identifying infrastructure elements that are digital or digitally enabled¹, and to assessing their security against known (current and emerging) cyber attacks and their overall resilience.**
- 2. Determinations regarding security against cyber attack against long-lasting infrastructure elements should take into account the quantum threat, as well as the need for quantum-safety and/or cryptographic agility.**
- 3. Cybersecurity should become another lens through which government views and judges the broad array of issues it faces.**

Points for Consideration:

- Quantum-Safe Canada supports the idea of a National Infrastructure Assessment and is pleased to provide comments on Infrastructure and Communities Canada's related engagement paper, *Building the Canada We Want in 2050*.
- There is an acknowledged gap between the infrastructure that Canada has and the infrastructure that we need, and there is broad acceptance that Canada must aim to 'build back better' when upgrading our national infrastructure stock.
- The engagement paper refers to an "ambition to build 21st century infrastructure" that will, presumably, rely heavily on digital elements including game-changing technologies like 5G wireless and lower-earth-orbit satellites (LEOs); however, the paper fails to acknowledge that such infrastructure must be designed and built to be cyber-secure.
- None of the three stated objectives of the initiative – promoting economic growth, tackling climate change, and improving social inclusion – can be achieved if the infrastructure we rely on has been rendered inoperable.
- The more critical the infrastructure, the more critical the cybersecurity. To use an example from the engagement paper, infrastructure assets related to Canada's "strategic trade corridors" – including roads, bridges, rail, airports and seaports – are heavily reliant on embedded digital elements that are prime targets of cyber attack.

¹ Here, 'digital infrastructure' refers to telecom, wireless and internet systems; 'digitally enabled infrastructure' refers to digital elements embedded in traditional 'heavy' infrastructure, e.g., sensors and actuators in smart bridges, roads and transit systems.

Building the *Cybersecure* Canada We Want in 2050

- We need to increase our ability to respond to increasingly sophisticated immediate threats to the cyber systems relied on by our critical infrastructure; these include ransomware attacks and organized reconnaissance and disruption activities by unfriendly nations and other malicious actors.
- Society must concurrently put in place the elements that will be required if we are to respond effectively to emerging, longer-term threats, perhaps the most pressing of which will be the threat to cryptography presented by quantum computing in the next decade or so.
- Quantum computing will bring about an almost unimaginable speed-up in the ability to perform calculations. Unfortunately, powerful quantum computers, while enabling wonderful advances in many areas, will also allow today's 'unbreakable' cryptography to be hacked in hours or minutes.
- The most common form of cryptography, that used in public-key infrastructure, is also the most vulnerable to quantum-based attack. This is a source of great concern, and Canada must respond proactively, putting in place measures that will support an orderly and timely transition to quantum-resistant cryptography.
- If we do not act, much of our critical infrastructure will become vulnerable to hostile actions because of weak cryptography. Due to the foundational nature of cryptography, failures will be systemic and devastating, and rapid recovery will be impossible.
- A standardised suite of viable quantum-resistant cryptographic systems is expected to be available in 2024, followed by a retooling of the ICT infrastructure worldwide, but this does not mean that proponents need to wait until then to take helpful steps.
- Proponents can safely design and build new digital or digitally enabled infrastructure now, provided they build in 'cryptographic agility' by installing modular units that can be accessed and replaced when the time comes.² This might also be called 'forward compatibility' or 'future-proofing'.
- Future-proofing is mentioned in the engagement paper in a slightly different sense in the context of data and new technologies, such as artificial intelligence, autonomous systems and machine learning. "The Assessment's work in these areas will allow infrastructure owners and funders to take advantage of the data and technologies available, and to 'future-proof' our infrastructure for generations to come."

² A simple analogy: Wall sockets provide electrical agility so that we don't have to rewire the house every time we buy a new lamp.

Building the *Cybersecure* Canada We Want in 2050

- Future-proofing efforts should also reflect an understanding that advanced digital systems such as artificial intelligence, autonomous systems and machine learning – like other digital infrastructure elements – will be vulnerable to the quantum threat if they haven't been made quantum-safe, or at least cryptographically agile.
- These considerations are of critical importance in terms of service continuity, national security and finance, and they are also important in terms of environmental sustainability, i.e., that projects are done correctly from the start.
- If infrastructure intended to improve sustainability stops working because it was improperly installed or insufficiently protected, then anticipated sustainability gains will be lost, resources will have been wasted, the financial cost of repair or replacement will divert funding from elsewhere, and additional resources will need to be deployed – each of which carries environmental costs.
- Beyond legislation and regulation, government has access to numerous policy powers that can help ensure that digitally enabled infrastructure is designed, built and installed to be cybersecure and quantum-safe.
- These levers include approval, planning, procurement and funding powers, none of which need be costly. Government could require proponents of infrastructure programs to provide acceptable cybersecurity strategies (including quantum-safe strategies) before receiving approval or funding.