Engineers Canada's submission to the House of Commons Standing Committee on Public Safety and National Security

Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts

Questions concerning the content of this brief should be directed to:

Joey Taylor
Manager, Public Affairs and Government Relations
Engineers Canada
joey.taylor@engineerscanada.ca
613.232.2474 Ext. 213

Overview

The Government of Canada is taking proactive measures to strengthen cybersecurity through comprehensive updates to *Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*. The proposed changes consist of two parts, each addressing specific aspects of cybersecurity.

Part 1 focuses on amending the *Telecommunications Act* to prioritize the security of the Canadian telecommunications system, while Part 2 introduces the *Critical Cyber Systems Protection Act* to safeguard critical cyber systems vital to national security and public safety.

By implementing these legislative changes, the federal government aims to enhance the security and resilience of the Canadian telecommunications system and critical cyber systems. These measures contribute to the overarching goal of creating a safer and more secure cyber environment within Canada, mitigating potential risks, and ensuring the protection of national interests.

Addressing cyber threats: safeguarding Canada's digital landscape

Cybersecurity is of utmost importance in our increasingly digital world, where the protection of computers, networks, software, and data from unauthorized access and malicious attacks is essential. Safeguarding Canada's critical infrastructure is key for economic stability and national security. Disruptions to essential infrastructure can result in catastrophic consequences, including loss of life, adverse economic effects, and damage to public confidence. As technology advances and digital systems become more complex, the skills of those seeking to exploit vulnerabilities also evolve. Cyberattacks and data breaches have become increasingly common, underscoring the need for robust cybersecurity measures.

The 2022 CIRA Cybersecurity Survey has shed light on the growing challenges faced by Canadian organizations in defending against cyber threats. The survey reveals a significant increase in the difficulty of warding off attacks compared to pre-pandemic times. Nearly 30 per cent of organizations experienced a data breach, while 15 per cent suffered reputational damage and loss of customers following an attack. These statistics underscore the urgent need for proactive cybersecurity measures.

Benefits of incorporating engineers in cybersecurity legislation

The involvement of licensed engineers, particularly those working in cybersecurity, is important for addressing these challenges effectively. Engineers possess expertise that makes them uniquely qualified to contribute to the design, implementation, and maintenance of cybersecurity measures. Their specialized knowledge, systems thinking approach, ethical accountability, adherence to rigorous

standards, and commitment to continuous professional development greatly benefit cybersecurity initiatives.

Ethical and professional accountability:

Engineers in specialized disciplines possess the same skills as other IT professionals but are held to a higher level of professional and ethical accountability through provincial and territorial legislation across Canada. Operating within a regulatory environment, engineers ensure accountability for their work. They adhere to stringent ethical and professional standards enforced by regulatory bodies, emphasizing best practices and public safety. By including engineers in federal legislation, cybersecurity initiatives benefit from their ethical accountability. This integration ensures the development, implementation, and maintenance of cybersecurity measures with a strong commitment to ethical conduct, accountability, and the protection of the public and the natural environment.

Specialized expertise:

Engineers possess specialized knowledge and skills that are highly relevant to cybersecurity. Their expertise in areas such as communications, system design, hardware, and software development equips them with a deep understanding of the technical aspects of cybersecurity. By involving engineers in the legislative process, the development and implementation of cybersecurity policies and regulations can benefit from their specialized insights, resulting in more effective and comprehensive cybersecurity measures.

Systems thinking and risk assessment:

Engineers are trained to approach problems from a systems perspective, considering the interdependencies and potential risks across various components. This holistic approach is invaluable when addressing cybersecurity challenges, as it enables engineers to assess vulnerabilities, identify potential attack vectors, and design mitigation strategies that consider the entire system. By incorporating engineers into the legislative process, policymakers can leverage their systems thinking abilities to develop comprehensive cybersecurity frameworks that account for the complexities of critical infrastructure.

Continual professional development:

Engineers are required to engage in continuous professional development to stay up-to-date with the latest industry trends, technologies, and best practices. By including engineers in federal legislation, cybersecurity initiatives can benefit from their commitment to ongoing education and knowledge acquisition. This equips them to address emerging cyber threats effectively, incorporating the latest defensive strategies and technologies into cybersecurity frameworks.

Recommendations

To ensure the involvement of engineers, Engineers Canada recommends the following amendments to the *Telecommunications Act*:

1. Amendment to Section 4(1) Subsection 71(2) Designation of Inspectors:
    - "(2) The Minister may designate any qualified person, such as a professional engineer, as an inspector for the purpose of verifying compliance or preventing non-compliance with the provisions of this Act for which the Minister is responsible. This includes orders made under section 15.1 and 15.2 or regulations made under paragraph 15.8(1)(a)."

This proposed amendment seeks to broaden the authority of the Minister to designate inspectors who are qualified individuals, such as professional engineers, for the specific purpose of ensuring compliance with the provisions of the Act. It enhances the effectiveness of enforcement mechanisms and strengthens the regulatory framework by empowering qualified inspectors to take appropriate measures to verify compliance and prevent non-compliance.

2. Amendment to Clause 4: (1) Existing text of subsection 71(2):
    - “(2) The Minister may designate any qualified person, such as a professional engineer as an inspector for the purpose of verifying compliance or preventing non-compliance with the provisions of this Act for which the Minister is responsible.”

The proposed amendment, which includes the addition of professional engineers as inspectors, acknowledges the specialized expertise they possess, which is of significant value in ensuring compliance with the Act and effectively preventing non-compliance. By granting the Minister the authority to designate professional engineers as inspectors, the amendment aims to enhance the effectiveness of inspections and enforcement activities by leveraging their technical knowledge and skills. This recognition of professional engineers' expertise will contribute to the overall effectiveness and efficiency of inspections, reinforcing the objective of upholding compliance with the Act.

Conclusion

The Committee's collaboration with key stakeholders, particularly the engineering profession, is crucial in supporting cybersecurity while upholding the public interest and public safety. By incorporating engineers into the legislative process, we can leverage their expertise and ensure the development of robust and resilient cybersecurity measures. Engineers Canada looks forward to contributing to these efforts and appreciates the Committee's consideration of the recommendations.

About Engineers Canada

Engineers Canada is the national organization that represents the 12 provincial and territorial engineering regulators that license the more than 300,000 members of the engineering profession in Canada. As the only national voice for the engineering profession, our organization has a long-standing history of working and collaborating with the federal government to help inform and develop legislation, regulations, and policies.