



Designated Operators: Interprovincial and International Pipeline Owners

This summer with the induction into Parliament of Bill C-26, an Act respecting cybersecurity with amendments to the Telecommunication Act with additional regulatory framework for cybersecurity through the Critical Cyber System Protection Act, pipeline operators will be responsible for increased reporting due to a new designation by the Federal Government as a Designated Operator.

The proposed bill will require Designated Operators of Interprovincial and International pipelines to increase their protection against cyber attacks. Designated Operators will be required to maintain a Cyber Security Program and make it available to Federal regulators. Designated Operators will be required to manage and identify cybersecurity risks and demonstrate mitigation activities. In addition, regular reviews will be required to validate systems maintain their protection against cyber attacks.

In the event of the cybersecurity incident, Designate Operators will be required to report the incident to the Communication Security Establishment and other Federal Regulators. While current legislation requires the reporting of unauthorized access and disclosure of personal information, the new legislation will require reporting in the event of an incident that interferes with the continuity or security of vital services or systems or the confidentiality, integrity or availability of critical systems.

Documentation requirements will also increase with companies designated as a Designate Operator will need to document steps that were taken to develop and implement a cybersecurity program, documenting all cybersecurity incidents and the steps taken to mitigate possible attacks.

Penalties under this new proposed legislation will be severe. Penalties will be \$1 million for an individual and \$15 million in any other case.

As the Federal Government takes steps to protect the digital infrastructure within Canada it is requiring more of companies operating in Canada to demonstrate their commitment to the same goal through action and documentation of the digital infrastructure companies operate.

Galaxy Broadband Communications can provide support in the development of cybersecurity programs, the documentation and reporting required to maintain a high vigilance that will be required to meet the legislative requirements. Galaxy can provide real time reporting and alerting to demonstrate the Federal Regulators that the requirements are being met and the processes that have been implemented are sustainable.

When clients begin to receive services from Galaxy, they understand the services they receive are different than other telecommunication providers. Galaxy provides a portfolio of communication services that are reliable and resilient. In addition, Galaxy understands the increasingly complex reporting frameworks that pipeline companies in Canada are now having to understand, implement and maintain their compliancy. In addition, Galaxy commits to meet with our client regularly to discuss current and potentially new services, incidents and issues that may have affected services.

Reach out to us through our website and click on the Ask an Expert button to start your new relationship with Galaxy for communication services, compliance reporting and portfolio management.

Galaxy Broadband Communications Inc.
4020A Sladeview Cres, Unit 4
Mississauga, ON L5L 6B1
Ph: 1.877.463.9728

