Q. (Reference Application Schedule B, Personal Computer Infrastructure, page 84 of 99) It is stated "*This project is justified on the obligation to provide reliable service to customers at least cost and cannot be deferred.*"

a) Please provide evidence based on reliability criteria that Newfoundland Power will be unable to provide reliable service at least cost if it were to delay this project.

b) Please quantify the impact on the following if the project were delayed by two years: 1) reliability, 2) cost, and 3) the risk and consequences of failure.

A. a) Newfoundland Power manages its capital expenditures in a manner that balances both the cost and reliability of the service provided to its customers.[1] The Company is focused on maintaining current levels of overall service reliability for its customers at the lowest possible cost.[2] The 2022 *Personal Computer Infrastructure*, *Shared Server Infrastructure* and *Network Infrastructure* projects are consistent with this objective.

Newfoundland Power maintains over 180 software applications in providing service to customers. Examples of these include the: (i) Supervisory Control and Data Acquisition ("SCADA") System used to monitor and control the electrical system; (ii) Outage Management System used to track and respond to customer outages; and (iii) Customer Service System used to respond to customer enquires and issue customer bills. The least-cost delivery of reliable service to customers is dependent upon the secure and reliable operation of these software applications.

The software applications used in providing service to customers operate on a combination of information technology ("IT") infrastructure. Server infrastructure provides the foundational hardware upon which applications operate. Personal Computer ("PC") infrastructure is used by employees to run the applications. Network infrastructure ensures connectivity among these devices throughout all Company-owned facilities and to the internet.[3]

Over time, component failures occur. The performance of IT infrastructure can also degrade as computing requirements and data transfer capabilities increase with the implementation of more advanced technologies.[4] Additionally, cybersecurity threats evolve over time, which threaten the secure operation of software applications.

[1] See response to Request for Information NLH-NP-042.

[2] See response to Request for Information CA-NP-014.

[3] Network infrastructure includes routers, firewalls and modems, among other components.

[4] As applications are upgraded or new applications are implemented, the amount of information transferred throughout the network between servers and PCs increases, which can result in reduced performance for software applications.

Newfoundland Power applies industry best practices to ensure the reliable operation of its IT infrastructure. The criteria applied by the Company in considering whether to replace or upgrade its IT infrastructure include:

(i) Identified performance, reliability or security issues. The Company monitors its PCs, servers and network components to identify issues with their operation. Infrastructure that consistently fails or experiences degraded reliability, performance or security is upgraded or replaced.[5]

(ii) Industry guidance on optimal technology lifecycles. Newfoundland Power currently achieves average lifecycles of 5 years for its PCs, compared to an industry average of 3 to 5 years.[6] The Company achieves average lifecycles for its servers of 7 years, compared to industry guidance of 5 to 6 years.[7] The average lifecycles for network components vary by component.[8] IT infrastructure is upgraded or replaced when it has exceeded its expected lifecycle and experiences reliability, performance or security issues.

(iii) Vendor support availability. Newfoundland Power maintains vendor supports for its servers and critical network components, such as routers and firewalls. This ensures that, should a failure or security issue occur, third-party expertise is available to resolve the issue. When this infrastructure becomes obsolete and is no longer supported by its vendor, an upgrade or replacement is required.

Applying these criteria ensures IT infrastructure can support the operation of software applications used in the day-to-day provision of service to customers.

Maintaining the Company's IT infrastructure through the 2022 *Personal Computer Infrastructure, Shared Server Infrastructure,* and *Network Infrastructure* projects is consistent with maintaining reliable service for customers at the lowest possible cost.

b) Delaying the 2022 *Personal Computer Infrastructure, Shared Server Infrastructure,* and *Network Infrastructure* projects by 2 years would extend IT infrastructure beyond its useful service life and increase the risk of failure. The primary consequences of

[5] For example, PCs, servers and network components have fans, internal storage, memory and other technology that wears and can fail over time.

[6] See *Recommended Life Spans to Guide Mobile, PC and Other Device Replacement Strategies*, Gartner Inc., March 31, 2021.

[7] See *Compute Infrastructure: How to Optimize the Management of Life Cycle Variations*, Gartner Inc., August 23, 2017.

[8] For example, industry guidance suggests an average lifecycle of 3 to 5 years for Wide Area Network ("WAN") edge computing, which provides connectivity between enterprise locations. Newfoundland Power achieves an average lifecycle of 7 to 9 years for this technology. Industry guidance also suggests an average lifecycle of 6 to 8 years for the Wireless Network ("Wi-Fi"). The Company's lifespan for this component falls within this range. See *Optimize Costs by Extending the Life Cycle of Campus and Branch Office Networking Equipment*, Gartner Inc., June 11, 2020.

failed IT infrastructure is reduced service reliability and increased costs to customers.[9]

For example, Newfoundland Power utilizes virtualized server environments wherein a single server hosts multiple software applications. The Company also operates Storage Area Networks ("SAN") that are critical to the effective operation of the server environment. If a server or SAN failed, the operation and performance of multiple software applications necessary to provide service to customers would be compromised. This includes software applications that are required to operate the electrical system, schedule, deploy and monitor field staff, and respond to customer enquiries.

Responding to in-service failures for IT infrastructure is generally more costly than responding to performance and reliability issues on a planned basis, particularly when issues occur outside of normal business hours.[10] Failures of PCs also increase the total cost of ownership and result in lost productivity among employees.[11]

Additionally, delaying these projects would expose customer and Company information to cybersecurity risks as threats evolve over time.[12]

Delaying the 2022 *Personal Computer Infrastructure, Shared Server Infrastructure,* and *Network Infrastructure* projects would therefore be inconsistent with maintaining reliable service for customers at the lowest possible cost.

[9] For information on Newfoundland Power's approach to quantifying risks and benefits, see response to Request for Information CA-NP-014.

[10] Responding to in-service failures outside of normal work hours requires higher labour costs and higher materials costs for any materials that are not readily available and require priority shipping.

[11] See *Use These Recommended Life Spans to Guide Mobile, PC and other Device Replacement Strategies,* Gartner Inc., September 5, 2019.

[12] For example, in 2019 the North American Electric Reliability Corporation ("NERC") reported that a vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices. See *Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities,* September 4, 2019. In May 2021, a ransomware attack forced the largest U.S. fuel pipeline to shut down for six days and led to gasoline shortages across several Southeastern states. See the Wall Street Journal, *Cyberattacks and Ransomeware: How Can We Protect Our Energy Infrastructure,* July 2021.