

August 20, 2025

Crystal Henwood
Clerk of the Board
Nova Scotia Energy Board
1601 Lower Water Street, 3rd Floor
Halifax, NS B3J 3S3

Re: M12273 – Nova Scotia Power’s Cybersecurity Incident - Monthly Update 1

Dear Ms. Henwood:

On July 14, 2025, the Nova Scotia Energy Board (NSEB, Board) directed Nova Scotia Power (NS Power, the Company) to file monthly progress reports about its response to the recent cybersecurity incident that impacted NS Power (Incident) and its progress in preparing the requested report about the Incident (Incident Report) with the initial progress report to be filed no later than August 1, 2025. For reasons noted in NS Power’s letter to the Board dated August 20, 2025, the filing of this report was delayed.

On April 25, 2025, NS Power identified a cybersecurity incident that resulted in unauthorized access to our information technology infrastructure. Upon detection of this activity, the Company immediately initiated containment, remediation and investigation efforts, engaging leading third-party cybersecurity experts and notifying the appropriate law enforcement authorities.

The Company has commenced the preparation of the Incident Report which will set out further details about these containment and remediation activities, the Company’s notice and transparency efforts, the steps taken to mitigate the potential harm to affected NS Power customers, and other content set out in the Board’s July 14, 2025 letter.

The Incident has not caused any disruption to physical operations at NS Power’s generation, transmission and distribution facilities, and the Incident has not impacted the Company’s ability to safely or reliably serve customers in Nova Scotia.

However, the Incident impacted some business systems housed in the Company’s data center, including those supporting enterprise resource planning, customer billing, energy trading, and underlying technology infrastructure such as servers, networks, and data storage.

To coordinate these efforts, we have established a Recovery Program Office to oversee and support the restoration of our business systems and processes. The Recovery Program Office is providing centralized leadership, ensuring alignment across workstreams, and facilitating decision-making as we progress through system restoration, infrastructure rebuilding, and the implementation of enhanced security measures. This coordinated approach allows us to efficiently manage resources, monitor risks, and maintain clear communication with end users, all while prioritizing the safe and secure return to full operational capability.

In addition, the Office of the Privacy Commissioner of Canada (OPC) has initiated an investigation into the Incident. The Company is fully cooperating with the OPC and is committed to addressing the OPC's concerns and resolving the investigation in an efficient and expeditious manner.

Yours truly,

A handwritten signature in blue ink, appearing to read "Judith Ferguson".

Judith Ferguson

Executive Vice President, Regulatory, Legal, and Government Relations