From: dt_macleod glenalpine.ca
To: Henwood, Crystal D
Subject: M12600 - Inquiry into Nova Scotia Power's Cybersecurity Incident
Date: March 27, 2026 2:32:36 PM

Good afternoon,

I'm writing to inform you of my application for Formal Intervenor Status concerning M12600 - Inquiry into Nova Scotia Power's Cybersecurity Incident. I am not a lawyer. I realize that my application is late. For this I apologize.

Could you guide me to the appropriate references for the creation of the brief.

I am a residential customer of Nova Scotia Power whose sensitive personal information was compromised in the April 2025 breach. My interest is distinct due to my professional background as a former Intelligence Analyst. My personal data potentially sets myself at risk for exploitation by state-sponsored or criminal actors.

I have already submitted the following to board@novascotia.ca:

Request for Formal Intervenor Status

To: Clerk of the Board, Nova Scotia Energy Board

Matter: M12600 - Inquiry into Nova Scotia Power's Cybersecurity Incident

Date: March 26, 2026

1. Intervenor Identification

Name: David Thomas MacLeod
Address: [redacted]

Contact:
Email: dt_macleod@glenalpine.ca
[redacted]

2. Nature of Interest

I am a residential customer of Nova Scotia Power whose sensitive personal information was compromised in the April 2025 breach. My interest is distinct due to my professional background as a former Intelligence Analyst. My personal data potentially sets myself at risk for exploitation by state-sponsored or criminal actors.

3. Issues to be Addressed

I intend to address the "Reasonableness of Nova Scotia Power's Preparedness" by analyzing

the gap between publicly available geopolitical threat assessments and NSP's security posture. Specifically:

a) The Forecasted Threat: How NSP's actions failed to align with the 2025-2026 National Cyber Threat Assessment warnings regarding Russian-nexus threats to critical infrastructure.

b) Data Retention Failures: Why NSP retained sensitive identifiers (SINs) for 540,000 customers despite these known risks, thereby unnecessarily expanding the "attack surface."

c) Detection Latency: The reasonableness of a 37-day delay (March 19 to April 25) in detecting a breach by a known geopolitical threat actor using established techniques.

4. Intention to Participate

I intend to:

a) File written evidence based on public intelligence assessments.

b) Submit Requests for Information (RfI's) to NSP regarding their threat-monitoring protocols.

c) Appear at the oral hearing on July 27, 2026, to provide testimony or cross-examine witnesses.

Sincerely,

David T MacLeod CD MA