IN THE MATTER OF: ***The Public Utilities Act***

– and –

IN THE MATTER OF:

AN INQUIRY about the impact of the cyber incident on **NOVA SCOTIA POWER INCORPORATED's** collection and retention of customer information, customer service and communications, billing processes and regulatory matters.

OPENING STATEMENT OF David MacLeod Public Interest Intervenor
August 14, 2026

Mr. Chair, Members of the Board:

My name is David MacLeod. I am before this tribunal today as a Public Interest Intervenor in Matter M12600. I served twenty-seven years in the Canadian Armed Forces, and during my service as an Intelligence Operator, I held a Top Secret clearance.

I've requested to become a public interest intervenor to add the perspective of over 75,000 Nova Scotians who have or have had a federal security reliability screening or clearance. This demographic includes public service employees, retirees and veterans, military personnel, research staff, and those working in the manufacturing of military equipment. Our intervention focuses specifically on the severe, long-term vulnerabilities created for this group due to the 2025 Nova Scotia Power cyber breach.

Usually, the public does not consider holding a security clearance to be a risk factor. However, in our information-saturated world, mosaic methods of intelligence collection and analysis make security clearance holders a uniquely vulnerable population. The compromise of Personally Identifiable Information (PII) does not merely expose clearance holders to standard commercial fraud. Instead, it hands foreign threat actors and criminal networks a permanent, weaponized mosaic of data to target, track, social-engineer, and blackmail clearance holders.

For an ordinary citizen, a data breach means an administrative headache and financial exposure. But security clearance holders must meet the demanding, and continuously intrusive vetting of the *Foreign Interference and Security of Information Act* (*FISIA*). The consequences of failing to meet requirements are severe and potentially career-ending.

Throughout this proceeding, we intend to demonstrate that standard corporate remedies are fundamentally inadequate for this demographic. Commercial credit monitoring flags whether someone opens a fraudulent credit card. It does not protect against dark-web dossier assembly, targeted spear-phishing, lifestyle profiling, or foreign coercion. A Social Insurance Number is static and lasts a lifetime; the dark web does not erase data after a few years. Offering a basic commercial credit report to an individual whose PII have been leaked to criminals or foreign intelligence entities is performative at best.

We look forward to cross-examining the witnesses to ensure proportional remedies are found to address the actual personal security and livelihood risks faced by Nova Scotian's who have or have had a federal access or security clearance

Thank you,

David MacLeod
Public Interest Intervenor M12600