**Form A – Information Requests**

M12600

**Nova Scotia Energy Board**

**In the Matter of:** ***THE PUBLIC UTILITIES ACT,*** **R.S.N.S. 1989, c.380, as amended**

**– and –**

**In the Matter of: AN INQUIRY** concerning 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

**Information Requests**
**Non-Confidential**

To: Nova Scotia Power Incorporated
Jennifer Power
Jennifer.Power@nspower.ca

From: David T. MacLeod

Responses due: Wednesday, May 6, 2026

Copies: 1 electronic copy (PDF searchable)
1 hard copies

Contact person: David T. MacLeod
[redacted]
dt_macleod@glenalpine.ca

Issued at Municipality of the County of Antigonish, Nova Scotia, this 9th day of April, 2026.

**Nova Scotia Energy Board**

TABLE OF CONTENTS

**Nova Scotia Energy Board**

## PREAMBLE AND INSTRUCTIONS TO RESPONDENT

**1.** These Information Requests (hereinafter "IRs" or "Interrogatories") are submitted pursuant to the Nova Scotia Energy Board Act, S.N.S. 2021, c. 3, and the Nova Scotia Energy Board Rules of Practice and Procedure, in connection with the Board's investigation into the cybersecurity incident identified by Nova Scotia Power Incorporated (NSP) on or about April 25, 2025, arising from an intrusion that commenced on or about March 19, 2025.

**2.** NSP is required to provide complete, accurate, and non-evasive responses to each Interrogatory. Where a response is withheld in whole or in part on grounds of commercial sensitivity, security, solicitor-client privilege, or other claimed protection, NSP shall:

(a) identify with specificity the information withheld;

(b) state the legal or regulatory basis for the claimed protection;

(c) provide a redacted or summary response to the greatest extent possible; and

(d) file a formal confidentiality application with the Board in accordance with the Board's established practice.

**3.** Where an Interrogatory calls for a document, policy, plan, procedure, report, assessment, audit, log, or communication, NSP shall produce the document(s) in their entirety, subject only to properly claimed and Board-approved confidentiality protections.

**4.** Where an Interrogatory asks NSP to "describe," "explain," or "identify," the response must be sufficiently detailed to enable a technically informed reader and the Board's independent expert (MNP Digital) to evaluate the adequacy of the measures described.

**5.** If NSP's position is that any Interrogatory is irrelevant, duplicative, unduly burdensome, or otherwise objectionable, NSP shall state that objection with full reasons and shall nonetheless provide such response as it is able to provide.

**6.** These IRs are not exhaustive. The right to file supplementary IRs arising from NSP's responses, or from documents produced in the course of this proceeding, is expressly reserved.

**DEFINITIONS**

For the purposes of these Interrogatories, the following definitions apply:

**"Advanced Persistent Threat" or "APT"** means a prolonged and targeted cyber intrusion in which an attacker establishes an undetected presence in a network in order to steal sensitive data, pre-position for disruption, or achieve other strategic objectives over an extended period.

**"AMI"** means Advanced Metering Infrastructure, including smart meters and the communications systems connecting those meters to NSP's billing and operational platforms.

**"Attack"** or **"Cybersecurity Incident"** means the ransomware intrusion that commenced on or about March 19, 2025, as described in NSP's Incident Report filed December 23, 2025 (Matter M12273).

**"BDR"** means Backup and Disaster Recovery infrastructure, including off-site data replication, redundant systems, and recovery procedures.

**"CCCS"** means the Canadian Centre for Cyber Security, the Government of Canada's technical authority on cybersecurity, operating as part of the Communications Security Establishment (CSE).

**"CISA"** means the United States Cybersecurity and Infrastructure Security Agency.

**"Critical Infrastructure"** has the meaning ascribed to it by the Government of Canada: processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, or economic well-being of Canadians and the effective functioning of government.

**"CSE"** means the Communications Security Establishment of Canada.

**"ICS"** means Industrial Control Systems, encompassing SCADA systems, distributed control systems (DCS), programmable logic controllers (PLCs), and related hardware and software used to monitor and control physical industrial processes.

**"Incident Report"** means NSP's formal Incident Report on the cybersecurity incident filed with the NSEB on December 23, 2025 (Matter M12273, redacted version publicly available).

**"IT"** means Information Technology, encompassing computing, networking, data storage, and software systems used for business administration, customer management, billing, communications, and related functions.

**"IT/OT Convergence"** means the integration of information technology (IT) systems with operational technology (OT) systems, and the associated cybersecurity risks arising from that integration.

**"NCTA"** means the National Cyber Threat Assessment published periodically by the CCCS, including the NCTA 2018, NCTA 2020, NCTA 2023-2024, and NCTA 2025-2026.

**"NERC CIP"** means the North American Electric Reliability Corporation Critical Infrastructure Protection standards, a set of mandatory cybersecurity standards applicable to the bulk electric system in North America.

**"NSEB"** means the Nova Scotia Energy Board.

**"NSP"** or **"NSPI"** means Nova Scotia Power Incorporated, a subsidiary of Emera Inc., and the respondent in these proceedings.

**"OT"** means Operational Technology, encompassing hardware and software systems used to monitor and control physical devices, processes, and events in industrial environments, including power generation, transmission, and distribution systems.

**"Ransomware"** means malicious software that encrypts a victim's data or systems and demands payment in exchange for restoration of access, and/or exfiltrates data and threatens its publication unless a ransom is paid.

**"Russian-Nexus Threat Actor"** means any cyber threat actor that is: (a) an organ of the Russian state, including but not limited to GRU-affiliated groups (e.g., Sandworm/ELECTRUM, APT28/Fancy Bear), FSB-affiliated groups (e.g., Turla), and SVR-affiliated groups (e.g., APT29/Cozy Bear); or (b) a criminal or hacktivist group operating with the knowledge, tolerance, permission, or direction of the Russian state, including but not limited to ransomware groups such as LockBit, BlackCat/ALPHV, Conti, and pro-Russia hacktivist collectives such as Killnet.

**"UARB"** means the Utility and Review Board, predecessor to the NSEB, before which NSP filed its IT-OT Cyber Security Control Implementation Phase 1 plan on February 27, 2025.

## EVIDENTIARY FOUNDATION AND DISCUSSION

### A. The Published Threat Landscape (2015–2025)

The following discussion summarizes the publicly available and authoritative threat intelligence that NSP, as a regulated critical infrastructure operator, knew or ought to have known prior to March 19, 2025. This discussion is provided to contextualize the Interrogatories that follow and to establish the evidentiary basis for the reasonableness standard applied.

A.1 Government of Canada Warnings and Situational Awareness — A Decade of Escalating Alerts

The CCCS has published a series of National Cyber Threat Assessments that, taken together, constitute an unambiguous and escalating warning to Canadian critical infrastructure operators, including electricity utilities, of the threat posed by Russian-nexus actors:

- **NCTA 2018** (Canadian Centre for Cyber Security, 2018): Identified state-sponsored actors, including Russia, as posing the most significant cyber threat to Canada's critical infrastructure. The NCTA 2018 warned of sophisticated intrusion campaigns targeting energy and other critical sectors, and identified pre-positioning for disruption as a key Russian strategic objective.
- **CCCS Electricity Sector Cyber Threat Bulletin** (Canadian Centre for Cyber Security, 2020): Dedicated specifically to Canada's electricity sector. Key judgements included: (a) state-sponsored actors were "very likely" engaged in espionage and pre-positioning within Canadian electricity sector networks; (b) cybercriminals were "increasingly likely" to target electricity sector ICS for extortion using customized ransomware; and (c) Russian-nexus hacktivist and state-sponsored actors posed a heightened threat following the invasion of Ukraine.
- **NCTA 2020** (Canadian Centre for Cyber Security, 2020): Warned that ransomware had become the most disruptive cybercrime threat to Canadian organizations and that state-sponsored actors continued to target critical infrastructure for espionage and pre-positioning.
- **NCTA 2023-2024** (Canadian Centre for Cyber Security, 2022): Identified critical infrastructure as "increasingly at risk" from both cybercriminal and state-sponsored actors.

Explicitly warned that Russian state-sponsored actors were targeting Canadian critical infrastructure in response to Canada's support for Ukraine.

- **NCTA 2025-2026** (Canadian Centre for Cyber Security, 2024): Published in October 2024 (five months before the Attack) this assessment explicitly identified Russian state-sponsored actors as posing a "very likely" (75-89%) threat to Canadian critical infrastructure, including the electricity sector. The NCTA 2025-2026 warned of: (a) pre-positioning by Russian-nexus actors within critical infrastructure networks for potential disruptive operations; (b) the use of ransomware by Russian-nexus criminal groups as a primary tool of disruption; (c) the convergence of state-sponsored and criminal cyber operations; and (d) the elevated threat to Canada arising from geopolitical tensions related to the Russia-Ukraine conflict and Canada's role as a NATO ally.
- **CCCS Oil and Gas Sector Cyber Threat Assessment** (Canadian Centre for Cyber Security, 2023): Extended the analysis of Russian-nexus threats to energy sector operators broadly, referencing the CISA Joint Advisory AA22-110A and CCCS bulletins on Russian threat activity related to the invasion of Ukraine.
- **Situational Awareness** Nova Scotia is central to Canada's defence posture, hosting major Canadian Armed Forces bases in Halifax and Greenwood. It also concentrates a large share of the defence industrial and research base, about 35% of Canada's defence companies, and NATO-linked innovation and research assets. Given these public, longstanding facts and the well-documented use of techniques such as phishing and spear-phishing against personnel handling sensitive information, a reasonable operator of critical infrastructure in Nova Scotia would be expected to recognize and account for this threat environment.

A.2 International Government and Alliance Warnings

- **CISA Joint Advisory AA22-110A** (CISA et al., 2022): Issued jointly by the cybersecurity authorities of the United States, Canada (CSE/CCCS), Australia, New Zealand, and the United Kingdom on April 20, 2022. This advisory explicitly warned that Russia's invasion of Ukraine could expose organizations "both within and beyond the region" to increased malicious cyber activity. It identified specific Russian-nexus APT groups, their tactics, techniques, and procedures (TTPs), and provided actionable mitigation guidance. Canada

was a co-signatory, making this advisory directly and authoritatively applicable to Canadian critical infrastructure operators.

- **NATO Cyber Defence Policy** (North Atlantic Treaty Organization, n.d.): NATO has progressively elevated cyber defence as a core collective defence obligation. The 2016 Warsaw Summit declared cyberspace a domain of operations. The 2022 Strategic Concept identified Russia as the most significant and direct threat to NATO security. Canada, as a NATO member, operates within this framework and its critical infrastructure operators are on notice of NATO's collective threat assessments.

A.3 Corporate Threat Intelligence

- **Dragos OT/ICS Cybersecurity Year in Review** (Dragos, Inc., 2024; 2025): Dragos, the leading industrial cybersecurity firm, tracked 26 active OT-focused threat groups as of 2025. Russian-nexus groups including ELECTRUM (Sandworm-affiliated), KAMACITE, and VOLTZITE were identified as actively targeting Western critical infrastructure, including electric utilities. Dragos reported that only 30% of OT networks had sufficient visibility to detect threats, and that 56% could not see below the IT/OT boundary, which was the vulnerability exploited in the NSP Attack.
- **IBM X-Force Threat Intelligence Index 2025** (IBM Security, 2025): Documented a 44% year-over-year increase in exploitation of public-facing applications and a significant increase in active ransomware groups. Energy and utilities remained among the most targeted sectors globally.

A.4 The Ukrainian Grid Attacks as Proof of Concept

The academic and technical literature establishes beyond reasonable dispute that Russian-nexus actors demonstrated both the capability and the intent to attack electricity infrastructure years before the NSP incident:

- **2015 BlackEnergy/Sandworm Attack**: GRU-affiliated Sandworm used the BlackEnergy malware to attack three Ukrainian distribution companies, causing approximately 225,000 customers to lose power — the first confirmed cyberattack to cause a power outage (Lee et al., 2016; Zetter, 2016).

- **2016 Industroyer/CRASHOVERRIDE Attack**: Sandworm deployed the Industroyer malware against the Ukrainian transmission grid, causing a one-hour blackout in Kyiv. Industroyer was the first malware specifically designed to attack industrial control systems in the electricity sector since Stuxnet (Cherepanov & Lipovsky, 2017; Dragos, Inc., 2017).
- **2022 Industroyer2 Attack**: Sandworm deployed an evolved variant, Industroyer2, against Ukrainian high-voltage substations, demonstrating continued development and deployment of grid-specific attack tools (ESET Research, 2022).

These attacks were extensively documented in open-source literature, government advisories, and corporate threat intelligence reports, which were publicly available to NSP.

**B. NSP's Acknowledged Risk and Inadequate Response**

The evidentiary record before the Board contains a critical and damaging admission. On **February 27, 2025** NSP's Chief Operating Officer, Dave Pickles, filed a report with the UARB titled *IT – OT Cyber Security Control Implementation Phase 1*, which explicitly acknowledged:

> "Organizations are subject to risk of external threats, and malicious and accidental insider threats. The volume and sophistication of cybersecurity threats against organizations is ever rising."

This filing demonstrates that NSP was on actual notice of the elevated and rising threat environment. However, the plan contained in that filing was:

1. **Exclusively OT-focused**: The plan addressed only operational technology systems (power generation, transmission, distribution). It did not address IT systems, customer data systems, billing platforms, or AMI infrastructure, which were the systems that were compromised in the Attack.
2. **Prospective and incomplete**: The plan described future implementation of cybersecurity controls, not existing capabilities. It acknowledged that NSP lacked a comprehensive cyber asset inventory for its OT environment as of that date.
3. **Silent on Russian-nexus threats**: Despite the NCTA 2025-2026 having been published five months earlier with explicit warnings about Russian-nexus threats to electricity utilities, the February 27, 2025 filing made no reference to that assessment or to the specific threat landscape it described.

Furthermore, the Halifax Examiner's reporting (Woodford, 2025) and NSP's own subsequent disclosures confirm:

- NSP did not detect the breach for **approximately 37 days** after the initial intrusion;
- NSP had **no operational Backup and Disaster Recovery (BDR) site** at the time of the Attack;
- NSP's billing systems remained impaired for **nearly one year** after the Attack;
- The threat actor **published stolen data**, including social insurance numbers, on the dark web;
- NSP's own Monthly Update 6 (March 2026) confirmed that virtual firewalls were being replaced with physical devices post-attack, which indicates that virtual firewalls, widely understood to be inadequate for critical infrastructure, were the primary boundary protection at the time of the Attack.

**C. The Standard of Reasonableness Applied**

The NSEB is asked to apply the standard of the **reasonably prudent regulated utility operator** in assessing NSP's preparedness. This standard requires that NSP:

1. **Monitor and act upon** publicly available threat intelligence from authoritative government and industry sources;
2. **Implement cybersecurity controls** commensurate with the identified threat level, including controls specifically recommended by CCCS, CISA, and applicable industry standards;
3. **Maintain adequate detection capabilities** sufficient to identify intrusions within a timeframe that limits harm;
4. **Protect customer data** with controls proportionate to the sensitivity of the information held;
5. **Maintain business continuity and disaster recovery capabilities** sufficient to restore critical services within a reasonable timeframe; and
6. **Comply with applicable regulatory frameworks** and industry standards, including NERC CIP where applicable.

The Interrogatories that follow are designed to elicit the evidence necessary for the Board and its independent expert (MNP Digital) to assess NSP's performance against each element of this standard.

## GROUP A — PRE-ATTACK THREAT AWARENESS AND GOVERNANCE

*These Interrogatories address NSP's governance structures, threat intelligence practices, and executive accountability for cybersecurity prior to March 19, 2025. They are grounded in the "knew or ought to have known" standard and NSP's acknowledged awareness of the threat environment.*

### IR A-1 — Threat Intelligence Program

(a) Did NSP maintain a formal threat intelligence program prior to March 19, 2025? If so, provide a complete description of that program, including:

  (i) the organizational unit responsible for threat intelligence;

  (ii) the sources of threat intelligence consulted (government, commercial, open-source, sector-sharing organizations such as E-ISAC);

  (iii) the frequency with which threat intelligence was reviewed and assessed;

  (iv) the process by which threat intelligence findings were escalated to senior leadership and the Board of Directors; and

  (v) the process by which threat intelligence findings were translated into cybersecurity control improvements.

(b) If NSP did not maintain a formal threat intelligence program prior to March 19, 2025, explain the basis on which NSP assessed the threat environment and made cybersecurity investment decisions.

(c) Did NSP seek to establish a partnership with the Communications Security Establishment to receive tailored threat intelligence, guidance, or technical assistance at any time between 2018 and March, 2025?

(d) Given the threat environment, the gaps in protection, and having situational awareness, did NSPI seek Minister of National Defence Ministerial Designation (a "system of importance") to access direct support from the Communications Security Establishment?

### IR A-2 — CCCS National Cyber Threat Assessments

(a) Confirm whether NSP reviewed each of the following CCCS publications prior to March 19, 2025:

(i) National Cyber Threat Assessment 2018;

(ii) CCCS Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector (November 2020);

(iii) National Cyber Threat Assessment 2020;

(iv) National Cyber Threat Assessment 2023-2024; and

(v) National Cyber Threat Assessment 2025-2026 (published October 2024).

(b) For each publication confirmed as reviewed:

(i) identify the individual(s) or organizational unit responsible for reviewing the publication;

(ii) describe the analysis conducted to assess the relevance of the publication's findings to NSP's specific threat environment;

(iii) describe any cybersecurity controls or improvements implemented by NSP in response to the findings of that publication; and

(iv) produce any internal memoranda, briefing notes, risk assessments, or board presentations prepared in response to the publication.

(c) For any publication not reviewed, explain why NSP did not review it and identify who, if anyone, was responsible for monitoring CCCS publications on behalf of NSP.

**IR A-3 — CISA Joint Advisory AA22-110A**

(a) Confirm whether NSP reviewed CISA Joint Cybersecurity Advisory AA22-110A, *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, issued April 20, 2022, and co-signed by Canada's Communications Security Establishment.

(b) If reviewed:

(i) describe the analysis conducted to assess the advisory's relevance to NSP's operations;

(ii) identify each of the specific mitigations recommended in the advisory and state whether NSP implemented each mitigation, and if so, when;

(iii) for any recommended mitigation not implemented, provide the documented rationale for non-implementation; and

(iv) produce all internal records related to NSP's review of and response to this advisory.

(c) If not reviewed, explain why NSP did not review an advisory co-signed by Canada's own cybersecurity authority and directed at critical infrastructure operators of which NSP is one.

**IR A-4 — Russian-Nexus Threat Awareness**

(a) Prior to March 19, 2025, did NSP's cybersecurity program specifically address the threat posed by Russian-nexus threat actors, including:

(i) GRU-affiliated groups (Sandworm/ELECTRUM, APT28);

(ii) FSB-affiliated groups (Turla, Berserk Bear/Dragonfly);

(iii) Russian-nexus ransomware groups (LockBit, BlackCat/ALPHV, Conti, and successors); and

(iv) pro-Russia hacktivist collectives (Killnet and affiliates)?

(b) If yes, describe the specific threat modelling, risk assessments, or scenario planning conducted with respect to each category of actor, and produce all related documentation.

(c) If no specific assessment was conducted for one or more categories, explain the basis on which NSP concluded that such an assessment was not required, having regard to the CCCS NCTA 2025-2026, the CISA Joint Advisory AA22-110A, and the CCCS Electricity Sector Bulletin, each of which specifically identified these actors as threats to electricity utilities.

**IR A-5 — Board of Directors and Executive Accountability**

(a) Describe the governance structure for cybersecurity at NSP prior to March 19, 2025, including:

(i) the role and responsibilities of the Chief Information Security Officer (CISO) or equivalent, and the reporting line of that position;

(ii) whether NSP had a dedicated CISO at the time of the Attack, and if not, who held equivalent responsibility;

(iii) the frequency and content of cybersecurity briefings provided to NSP's Board of Directors or its relevant committee;

(iv) the frequency and content of cybersecurity briefings provided to NSP's Executive Leadership Team; and

(v) the most recent cybersecurity risk assessment presented to NSP's Board prior to March 19, 2025, and the date of that presentation.

(b) Produce all Board of Directors and Executive Leadership Team meeting minutes, presentations, and briefing notes related to cybersecurity from January 1, 2022 to March 19, 2025.

(c) Produce NSP's cybersecurity risk register, or equivalent document, as it existed immediately prior to March 19, 2025.

**IR A-6 — The February 27, 2025 UARB Filing**

(a) NSP's Chief Operating Officer filed a report titled *IT – OT Cyber Security Control Implementation Phase 1* with the UARB on February 27, 2025, twenty days before the Attack. With respect to that filing:

(i) Explain why the plan was limited to OT systems and did not address IT systems, customer data systems, billing platforms, or AMI infrastructure;

(ii) Identify who reviewed and approved the scope of that plan prior to filing;

(iii) Describe what cybersecurity controls were in place for IT systems, customer data systems, and billing platforms as of February 27, 2025, if those systems were excluded from the plan;

(iv) Confirm whether the NCTA 2025-2026 was considered in the preparation of that plan, and if not, explain why;

(v) Identify any risk assessment that evaluated the cybersecurity of IT and customer data systems as of February 27, 2025; and

(vi) Produce all drafts, internal reviews, and approval records related to that filing.

(b) Having acknowledged in that filing that "the volume and sophistication of cybersecurity threats against organizations is ever rising," explain what specific steps NSP took between February 27, 2025 and March 19, 2025 to address the identified risk.

## GROUP B — IT/OT ARCHITECTURE AND NETWORK SEGMENTATION

*These Interrogatories address the technical architecture of NSP's IT and OT environments, the degree of segmentation between them, and the vulnerability of NSP's systems to the attack vector used. They are grounded in the well-documented finding that inadequate IT/OT segmentation is the primary enabler of ransomware attacks on utilities.*

### IR B-1 — Network Architecture Documentation

(a) Produce a network architecture diagram depicting NSP's IT and OT environments as they existed on March 18, 2025 (the day before the Attack), including:

  (i) the boundaries between IT and OT networks;

  (ii) all network segmentation controls (firewalls, DMZs, data diodes, unidirectional gateways);

  (iii) all external-facing access points, including remote access infrastructure;

  (iv) the location and connectivity of AMI systems, billing platforms, customer information systems, and financial systems within the network architecture; and

  (v) all connections to third-party systems, vendors, and managed service providers.

(b) NSP may apply for confidential treatment of this document. However, NSP shall provide a summary description sufficient to enable the Board and MNP Digital to assess the adequacy of the architecture.

### IR B-2 — IT/OT Segmentation

(a) Describe the segmentation controls that existed between NSP's IT and OT networks as of March 18, 2025.

(b) NSP's Monthly Update 6 (March 2026) disclosed that post-attack remediation included "the continued replacement of virtual firewalls with physical devices." Confirm:

  (i) that virtual firewalls were the primary boundary protection between IT and OT networks at the time of the Attack;

  (ii) the specific virtual firewall products in use;

(iii) whether NSP was aware, prior to the Attack, that the cybersecurity community and CISA had identified virtual firewalls as insufficient boundary protection for critical infrastructure OT environments; and

(iv) the date on which the decision was made to replace virtual firewalls with physical devices, and whether this decision was made in response to the Attack or had been planned prior to the Attack.

(c) Describe the specific attack path used by the threat actor, to the extent determined through NSP's forensic investigation, and identify the segmentation controls, if any, that failed to contain the intrusion.

**IR B-3 — Remote Access Infrastructure**

(a) Describe all remote access mechanisms in use at NSP as of March 18, 2025, including:

(i) VPN solutions, including vendor, version, and patch level;

(ii) Remote Desktop Protocol (RDP) exposure, including whether RDP was accessible from the internet;

(iii) third-party remote access tools used by vendors, managed service providers, or contractors; and

(iv) multi-factor authentication (MFA) implementation status for each remote access mechanism.

(b) CISA Joint Advisory AA22-110A (2022), co-signed by Canada's CSE, specifically identified insecure remote access as a primary attack vector exploited by Russian-nexus threat actors and directed critical infrastructure operators to "secure and monitor Remote Desktop Protocol and other risky services." Confirm whether NSP implemented each of the remote access mitigations specified in that advisory prior to March 19, 2025, and if not, explain why.

(c) Identify whether the initial intrusion vector in the Attack involved a remote access mechanism, and if so, specify which mechanism.

**IR B-4 — Third-Party and Supply Chain Risk**

(a) Identify all third-party vendors, managed service providers, and contractors with network access to NSP's IT or OT environments as of March 18, 2025.

(b) Describe NSP's third-party cybersecurity risk management program as it existed prior to the Attack, including:

(i) vendor cybersecurity assessment requirements;

(ii) contractual cybersecurity obligations imposed on third parties;

(iii) monitoring of third-party access; and

(iv) the most recent third-party security audit conducted prior to the Attack.

(c) Confirm whether the Attack involved any third-party access vector, and if so, identify the third party involved and describe the nature of the access.

**IR B-5 — AMI and Smart Meter Infrastructure**

(a) Describe the cybersecurity architecture of NSP's AMI system as of March 18, 2025, including the network connectivity between field devices, head-end systems, and billing platforms.

(b) The Attack resulted in approximately 450,000 smart meters losing their connection to NSP's billing platform, with full reconnection not achieved until March/April 2026. Explain:

(i) why the ransomware was able to affect AMI connectivity;

(ii) what segmentation controls existed between the AMI system and the affected IT systems;

(iii) whether NSP had conducted a cybersecurity risk assessment of the AMI system prior to the Attack; and

(iv) whether the AMI system was included in NSP's February 27, 2025 IT-OT Cyber Security Control Implementation Phase 1 plan.

## GROUP C — THREAT DETECTION AND INCIDENT RESPONSE

*These Interrogatories address NSP's capability to detect intrusions and respond to cybersecurity incidents. The 37-day detection gap — from initial intrusion on March 19, 2025 to NSP's awareness in late April 2025 — is a central issue in this proceeding.*

### IR C-1 — Security Monitoring and Detection Capabilities

(a) Describe NSP's security monitoring and threat detection capabilities as they existed on March 18, 2025, including:

  (i) Security Information and Event Management (SIEM) systems in use, including vendor, version, and scope of coverage;

  (ii) Endpoint Detection and Response (EDR) solutions deployed, and the percentage of endpoints covered;

  (iii) Network Detection and Response (NDR) capabilities;

  (iv) OT-specific monitoring tools (e.g., Dragos Platform, Claroty, Nozomi Networks);

  (v) Security Operations Centre (SOC) capabilities, whether in-house, outsourced, or hybrid, and hours of operation; and

  (vi) any managed detection and response (MDR) service in use.

(b) Dragos's 2025 OT Cybersecurity Year in Review reported that only 30% of OT networks had sufficient visibility to detect threats before operational impact, and that 56% of organizations could not see below the IT/OT boundary. Describe whether NSP's monitoring capabilities provided visibility below the IT/OT boundary, and if not, why that gap was not addressed prior to the Attack.

(c) Produce all security monitoring architecture documentation, SOC service agreements, and detection coverage assessments as they existed prior to March 19, 2025.

### IR C-2 — The 37-Day Detection Gap

(a) Provide a detailed forensic timeline of the Attack from initial intrusion to NSP's awareness, including:

  (i) the date and method of initial access;

(ii) the lateral movement path taken by the threat actor within NSP's network;

(iii) the date on which data exfiltration commenced;

(iv) the date on which ransomware was deployed;

(v) the date on which NSP's systems first generated alerts or indicators of compromise; and

(vi) the date on which NSP became aware of the intrusion and the source of that awareness (i.e., internal detection or third-party notification).

(b) Explain why NSP's existing detection capabilities failed to identify the intrusion for approximately 37 days.

(c) Identify all security alerts, anomaly detections, or indicators of compromise generated by NSP's systems between March 19, 2025 and late April 2025, and explain how each was handled by NSP's security team.

**IR C-3 — Incident Response Plan**

(a) Did NSP have a formal Cybersecurity Incident Response Plan (IRP) in place prior to March 19, 2025? If so, produce the most recent version of that plan as it existed prior to the Attack.

(b) Describe whether the IRP specifically addressed:

(i) ransomware attacks;

(ii) attacks by Russian-nexus state-sponsored or criminal actors;

(iii) attacks affecting both IT and OT environments simultaneously;

(iv) data exfiltration and the threat of data publication; and

(v) regulatory notification obligations, including obligations to the NSEB, the Office of the Privacy Commissioner of Canada, and law enforcement.

(c) Describe the most recent tabletop exercise or incident response drill conducted prior to the Attack, including the date, scenario used, participants, and findings.

(d) Identify any findings or recommendations from previous incident response exercises or third-party assessments that had not been implemented at the time of the Attack, and explain why implementation had not occurred.

**IR C-4 — Regulatory and Law Enforcement Notification**

(a) Provide a complete timeline of NSP's notifications to regulatory and law enforcement bodies following discovery of the Attack, including:

  (i) notification to the NSEB / UARB;

  (ii) notification to the Office of the Privacy Commissioner of Canada;

  (iii) notification to the CCCS;

  (iv) notification to the RCMP or other law enforcement agencies; and

  (v) notification to customers.

(b) Identify the regulatory and legal obligations that governed each notification requirement, and confirm whether NSP met each obligation within the required timeframe.

(c) Describe the basis on which NSP determined that no ransom payment would be made, including the sanctions analysis conducted and the law enforcement guidance received.

## GROUP D — CUSTOMER DATA PROTECTION AND PRIVACY GOVERNANCE

*These Interrogatories address NSP's obligations to protect customer personal information, including sensitive financial data and social insurance numbers, and the adequacy of NSP's data governance practices prior to the Attack.*

### IR D-1 — Data Inventory and Classification

(a) Produce NSP's data inventory or data map as it existed prior to March 19, 2025, identifying:

  (i) all categories of personal information held by NSP;

  (ii) the systems in which each category of personal information was stored;

  (iii) the retention periods applied to each category; and

  (iv) the access controls applied to each category.

(b) Explain why NSP held social insurance numbers (SINs) for customers, given that SINs are not required for the provision of electricity services, and describe the legal basis and business justification for collecting and retaining SINs.

(c) Describe the data minimization practices applied by NSP prior to the Attack.

### IR D-2 — Data Protection Controls

(a) Describe the technical and organizational controls applied to protect customer personal information prior to March 19, 2025, including:

  (i) encryption of personal information at rest and in transit;

  (ii) access controls and privileged access management for systems containing personal information;

  (iii) data loss prevention (DLP) tools or controls; and

  (iv) monitoring for unauthorized access to or exfiltration of personal information.

(b) The CCCS NCTA 2025-2026 explicitly warned that ransomware groups operating with Russian-nexus connections commonly engage in double-extortion tactics — encrypting data and threatening publication. Describe what specific controls NSP had implemented to prevent or detect data exfiltration prior to the Attack, having regard to this warning.

(c) Describe the most recent privacy impact assessment (PIA) conducted by NSP prior to the Attack, including the date, scope, and findings of that assessment.

**IR D-3 — Scope of Customer Data Compromise**

(a) Provide a complete accounting of the personal information stolen in the Attack, including:

(i) the total number of customers affected;

(ii) the categories of personal information stolen (name, address, email, bank account information, SIN, other);

(iii) the number of customers whose SINs were compromised;

(iv) the date on which the stolen data was published by the threat actor; and

(v) the steps taken by NSP to have the data removed from public access.

(b) Explain why NSP was not aware that its data had been exfiltrated until a third party notified NSP in late April 2025, and describe what data exfiltration detection controls, if any, were in place at the time.

## GROUP E — BACKUP, DISASTER RECOVERY, AND BUSINESS CONTINUITY

*These Interrogatories address NSP's backup and disaster recovery capabilities, which the evidence establishes were wholly inadequate at the time of the Attack. The near-year-long disruption to billing systems is directly attributable to the absence of an operational BDR site.*

### IR E-1 — Backup and Disaster Recovery Infrastructure

(a) Describe NSP's backup and disaster recovery infrastructure as it existed on March 18, 2025, including:

  (i) the backup solutions in use for each critical system (billing, AMI, financial, OT);

  (ii) the frequency and scope of backups;

  (iii) whether backups were stored offline, off-site, or in an air-gapped environment;

  (iv) the most recent backup restoration test conducted for each critical system, and the results of that test; and

  (v) whether NSP had an operational off-site BDR site.

(b) NSP's Monthly Update 6 (March 2026) disclosed that a BDR site was built and made operational post-attack. Confirm that NSP did not have an operational off-site BDR site at the time of the Attack, and explain why the construction of such a site had not been completed prior to March 19, 2025, having regard to:

  (i) the CCCS NCTA 2025-2026 warning that ransomware was a primary threat to critical infrastructure;

  (ii) the Colonial Pipeline ransomware incident of May 2021, which demonstrated the operational impact of ransomware on critical energy infrastructure; and

  (iii) industry best practices and CCCS guidance on ransomware resilience.

(c) Produce NSP's Business Continuity Plan and Disaster Recovery Plan as they existed prior to March 19, 2025.

### IR E-2 — Recovery Time and Business Impact

(a) Provide a complete timeline of NSP's recovery efforts from March 19, 2025 to the present, including:

  (i) the date on which each critical system was restored to full functionality;

(ii) the number of customers receiving estimated rather than actual bills in each month from May 2025 to April 2026;

(iii) the total number of customers who may have been overcharged as a result of estimated billing; and

(iv) the total financial cost to NSP of the Attack, including remediation, recovery, third-party expert fees, customer notification, credit monitoring, regulatory proceedings, and any other related costs.

(b) Explain the basis on which NSP seeks to recover any costs associated with the Attack through regulated rates, having regard to the finding that NSP's preparedness was inadequate.

## GROUP F — REGULATORY COMPLIANCE AND INDUSTRY STANDARDS

*These Interrogatories address NSP's compliance with applicable cybersecurity standards and regulatory frameworks, including NERC CIP, NIST CSF, and CCCS guidance.*

### IR F-1 — NERC CIP Compliance

(a) Identify which, if any, of NSP's assets are classified as Bulk Electric System (BES) Cyber Systems subject to mandatory NERC CIP standards.

(b) For each applicable NERC CIP standard (CIP-002 through CIP-014), describe NSP's compliance status as of March 18, 2025, including:

  (i) the most recent compliance audit conducted;

  (ii) any findings of non-compliance or areas of concern identified in that audit; and

  (iii) remediation actions taken in response to any findings.

(c) If NSP's assets are not subject to mandatory NERC CIP standards, explain the regulatory framework that governed NSP's cybersecurity obligations and describe how NSP ensured that its cybersecurity practices were commensurate with NERC CIP standards as a matter of best practice.

### IR F-2 — NIST Cybersecurity Framework

(a) Describe NSP's adoption of the NIST Cybersecurity Framework (CSF) or equivalent framework prior to March 19, 2025.

(b) Produce any maturity assessments conducted against the NIST CSF or equivalent framework in the three years prior to the Attack.

(c) For each of the five NIST CSF functions (Identify, Protect, Detect, Respond, Recover), describe NSP's self-assessed maturity level as of March 18, 2025, and identify any gaps identified and the remediation planned.

**IR F-3 — Third-Party Cybersecurity Assessments**

(a) Identify all third-party cybersecurity assessments, audits, penetration tests, vulnerability assessments, or red team exercises conducted for NSP in the five years prior to the Attack, including:

(i) the name of the third-party firm;

(ii) the scope and date of each assessment;

(iii) the key findings and recommendations; and

(iv) NSP's response to each finding, including whether and when each recommendation was implemented.

(b) Produce all third-party cybersecurity assessment reports from the five years prior to the Attack.

(c) Identify any findings from those assessments that remained unaddressed at the time of the Attack, and explain why those findings had not been remediated.

**IR F-4 — Cybersecurity Investment and Resource Allocation**

(a) Provide NSP's cybersecurity budget for each of the five fiscal years prior to the Attack (2020–2024), including:

(i) total cybersecurity expenditure;

(ii) allocation between IT security and OT security;

(iii) staffing levels in cybersecurity roles; and

(iv) capital expenditures on cybersecurity infrastructure.

(b) Describe any requests made by NSP's cybersecurity team for additional resources, funding, or staffing in the three years prior to the Attack that were not approved, and identify who made the decision not to approve those requests.

(c) Describe how NSP benchmarked its cybersecurity investment against peer utilities and industry best practices.

## GROUP G — POST-INCIDENT REMEDIATION AND FORWARD COMMITMENTS

*These Interrogatories address NSP's post-attack remediation program, the adequacy and pace of that program, and NSP's forward commitments to prevent recurrence. They are relevant to both the Board's assessment of NSP's ongoing accountability and to the question of whether ratepayers should bear the costs of remediation.*

### IR G-1 — Remediation Program Scope and Governance

(a) Produce NSP's complete post-incident remediation roadmap, including:

  (i) all remediation initiatives identified;

  (ii) the status of each initiative as of the date of filing;

  (iii) target completion dates for each initiative;

  (iv) the estimated cost of each initiative; and

  (v) the governance structure overseeing the remediation program.

(b) Describe the process by which NSP determined the scope of its remediation program, including whether that process involved a comprehensive gap analysis against the NCTA 2025-2026, CISA AA22-110A, NERC CIP, NIST CSF, and Dragos/IBM X-Force threat intelligence findings.

### IR G-2 — Specific Remediation Measures

For each of the following remediation measures referenced in NSP's Monthly Updates or Incident Report, provide the current status, target completion date, and estimated cost:

(a) Replacement of virtual firewalls with physical devices;

(b) Construction and operationalization of the off-site Backup and Disaster Recovery (BDR) site;

(c) Restoration of AMI meter-to-billing platform connectivity for all customers;

(d) Implementation of enhanced network segmentation between IT and OT environments;

(e) Deployment of OT-specific monitoring and detection capabilities;

(f) Implementation or enhancement of privileged access management;

(g) Implementation or enhancement of multi-factor authentication across all systems;

(h) Enhanced employee cybersecurity awareness training;

(i) Review and update of the Cybersecurity Incident Response Plan; and

(j) Engagement of a third-party managed detection and response (MDR) provider.

**IR G-3 — Attribution and Threat Actor Identification**

(a) NSP's Monthly Update 6 (March 2026) and related reporting attributed the Attack to "Russian threat actors." Provide all information available to NSP regarding the attribution of the Attack, including:

  (i) the identity of the threat actor or ransomware group, to the extent determined;

  (ii) the attribution methodology used;

  (iii) whether the threat actor is a Russian-nexus ransomware group, a state-sponsored APT, or both;

  (iv) whether any law enforcement agency has confirmed or supplemented NSP's attribution; and

  (v) whether the threat actor is subject to Canadian, U.S., or international sanctions, and the implications of that for any ransom payment analysis.

(b) Describe how knowledge of the threat actor's identity has informed NSP's remediation program and forward cybersecurity strategy.

**IR G-4 — Cost Recovery and Ratepayer Implications**

(a) Identify all costs associated with the Attack and its remediation that NSP intends to seek to recover through regulated rates, including:

  (i) the total quantum of costs to be sought;

  (ii) the regulatory basis for each category of cost recovery; and

  (iii) the allocation of costs between capital and operating expenditure.

(b) Describe NSP's position on whether the costs of the Attack should be borne by ratepayers, having regard to:

  (i) the finding that NSP acknowledged the risk of a cyber attack in its February 27, 2025 UARB filing;

(ii) the finding that NSP's IT systems and customer data were not included in NSP's cybersecurity plan at the time of the Attack;

(iii) the availability of comprehensive public threat intelligence that would have enabled NSP to implement adequate controls prior to the Attack; and

(iv) the principle that regulated utilities should not be permitted to recover costs arising from their own unreasonable conduct.

(c) Identify whether NSP maintained cybersecurity insurance at the time of the Attack, the coverage limits and scope of that insurance, and the amount of any insurance recovery received or expected.

**IR G-5 — Forward Cybersecurity Strategy**

(a) Produce NSP's updated cybersecurity strategy, policy, and multi-year investment plan, as approved by NSP's Board of Directors following the Attack.

(b) Describe how NSP's forward cybersecurity strategy addresses the specific warnings contained in the CCCS NCTA 2025-2026 regarding Russian-nexus threats to Canadian electricity utilities.

(c) Describe the mechanisms NSP has put in place to ensure that future CCCS, CISA, and allied-nation threat advisories are reviewed, assessed for relevance, and acted upon in a timely manner.

(d) Describe NSP's plan for participation in sector-specific cybersecurity information sharing organizations, including the Electricity Information Sharing and Analysis Centre (E-ISAC) and any Canadian equivalents.

**REFERENCES**

Canadian Centre for Cyber Security. (2018). *National cyber threat assessment 2018*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018

Canadian Centre for Cyber Security. (2020a). *Cyber threat bulletin: The cyber threat to Canada's electricity sector*. Government of Canada. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector

Canadian Centre for Cyber Security. (2020b). *National cyber threat assessment 2020*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020

Canadian Centre for Cyber Security. (2022). *National cyber threat assessment 2023-2024*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

Canadian Centre for Cyber Security. (2023). *The cyber threat to Canada's oil and gas sector*. Government of Canada. https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector

Canadian Centre for Cyber Security. (2024). *National cyber threat assessment 2025-2026*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Cherepanov, A., & Lipovsky, R. (2017). *Industroyer: Biggest threat to industrial control systems since Stuxnet*. ESET Research. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, Australian Cyber Security Centre, Canadian Centre for Cyber Security, National Cyber Security Centre (New Zealand), & National Cyber Security Centre (United Kingdom). (2022, May 9). *Russian state-sponsored and criminal cyber threats to critical infrastructure* (Alert AA22-110A). CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

Dragos, Inc. (2024). *2023 year in review: OT cybersecurity*. Dragos. https://www.dragos.com/year-in-review/

Dragos, Inc. (2025). *2024 OT cybersecurity year in review*. Dragos. https://www.dragos.com/year-in-review/

ESET Research. (2022, April 12). *Industroyer2: Industroyer reloaded*. ESET. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Henderson, J. (2026, March 6). Nova Scotia Power cyber update reveals continuing fallout. *Halifax Examiner*. https://www.halifaxexaminer.ca/economy/utilities/nova-scotia-power-cyber-update-reveals-continuing-fallout/

IBM Security. (2025). *IBM X-Force threat intelligence index 2025*. IBM. https://www.ibm.com/reports/threat-intelligence

Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid*. SANS ICS and Electricity Information Sharing and Analysis Center (E-ISAC). https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

North Atlantic Treaty Organization. (n.d.). *Cyber defence*. NATO. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

North Atlantic Treaty Organization. (2022). *NATO 2022 strategic concept*. NATO. https://www.nato.int/cps/en/natohq/topics_210907.htm

Nova Scotia Energy and Regulatory Boards Tribunal. (2025, May 15 – 2026, March 6). *Investigation log: Board inquiry into NS Power cyber incident* (Matter M12273). https://nserbt.ca/nseb/news/investigation-log-board-inquiry-ns-power-cyber-incident-1

Nova Scotia Energy and Regulatory Boards Tribunal. (2026, February 6). *Board letter outlining preliminary scope of issues in matters M12273 and M12600*. https://nserbt.ca/sites/default/files/M12273%20and%20M12600%20-%20Board%20Letter.pdf

Nova Scotia Power Inc. (2025, February 27). *IT – OT cyber security control implementation phase 1* [Report filed with the Utility and Review Board]. Nova Scotia Utility and Review Board.

Nova Scotia Power Inc. (2025, December 23). *Incident report on cybersecurity incident* (Matter M12273, redacted). https://nserbt.ca/sites/default/files/M12273%20-%20Incident%20Report%20%28redacted%29.pdf

Nova Scotia Power Inc. (2026, March 6). *Monthly update 6 on cybersecurity incident* (Matter M12273). https://nserbt.ca/sites/default/files/Monthly%20Update%206.pdf

Woodford, Z. (2025, May 30). Nova Scotia Power saw the potential for a cyber attack, but did too little too late. *Halifax Examiner*. https://www.halifaxexaminer.ca/morning-file/nova-scotia-power-saw-the-potential-for-a-cyber-attack-but-did-too-little-too-late/

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/