Request IR C-4:

(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.

Response IR C-4:

(a) See Section 4.2 and 4.3 of the Incident Report for details on NS Power's notifications to the above noted stakeholders and regulatory bodies. NS Power notified the NSEB of system interruptions on April 25, 2025 and definitively on April 28, 2025.

(b) Under PIPEDA, organizations have an obligation to report to the OPC, and notify affected individuals of any breach of security safeguards involving personal information under its control where the incident meets the required threshold. Under PIPEDA, the

report to the OPC, and notifications to impacted customers must be made "as soon as feasible after the organization determines that the breach has occurred". See Section 4.3 of the Incident Report for information on NS Power's notification and reporting timeline. Notifications to the NSEB, UARB, CCCS, and to law enforcement were made in alignment with NS Power's established incident response protocols. NS Power does not have a specific regulatory or legal obligation to report cyber incidents to these entities.

Request IR D-1:

(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.

Response IR D-1:

(a) See responses to NSEB IR-9, INQ IR-1, 2, and 4 for information on the categories of personal information held by NS Power, and the relevant protections and retention periods.

(b) Please see Section 8.5 of the Incident Report.

(c) Please see the response to NSEB IR-9, and INQ IR-1 and 2 for details on NS Power's privacy program.

Request IR D-2:

(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.

Response IR D-2

(a) See Section 8.1 of the Incident Report for details on NS Power's cybersecurity standards and policies. At the time of the Incident, NS Power had implemented a common set of cybersecurity standards and policies that are informed, in part, by the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, and the Company regularly reviews and makes continuous improvements to its cybersecurity programs to ensure it is in line with the latest guidance. These practices include encryption practices, access controls, data loss prevention tools, and monitoring practices.

(b) Please see response to (a).

(c) See the response to NSEB IR-9 for details on NS Power's privacy program.

Request IR D-3:

(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.

Response IR D-3:

(a) Please see Section 2.0 of the Incident Report for details on the impacted data.

(b) Please see Section 2.0 of the Incident Report for a timeline setting out the discovery of the Incident.

Request IR E-2:

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

(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.

Response IR E-2:

(a) Please refer to NSPI to NSEB – Cybersecurity Incident Monthly updates 1-7 for a timeline of recovery efforts.

(ii)

Month	Bills Estimated
May-25	2387
Jun-25	491994
Jul-25	206762
Aug-25	136366
Sep-25	180222
Oct-25	160523
Nov-25	179001
Dec-25	157290
Jan-26	52353
Feb-26	25771
Mar-26	17926
Apr-26	4978

(iii) Actual overpayment and underpayment scenarios resultant from estimates are difficult to isolate, as trued-up usage cannot be ascribed to the date of use.