

NON-CONFIDENTIAL

Request IR A-6:

(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;

Response IR A-6:

(a)

(i) The IT systems were subject to a separate cybersecurity control implementation plan, which began in 2021 and remained ongoing at the time of the cyber incident in 2025. IT systems, customer data systems, billing platforms and AMI infrastructure are on the Corporate IT network and were part of that separate plan.

(ii) The scope of the OT Cyber Security Control Implementation phase 1 had been defined by Deloitte LLP and approved by NS Power’s Director of Information Security and Risk Management.

NON-CONFIDENTIAL

Request IR B-4:

(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.

Response IR B-4:

That source data was lost as part of the cyber incident and is no longer available. But as a normal course of business, NS Power relies on third parties, and where necessary and with appropriate cyber safeguards, those third parties are granted limited access to systems required to perform their duties.