STAKEHOLDER RESPONSES – INTERIM CYBER SECURITY PROCEDURE V1.0

Item	Section	Submission	Comment	ISO Response
1.	2.1.1	Alinta	The procedure places obligations on: • Covered Networks; • The ISO Control Desk; • Registered NSPs that are not excluded networks or an integrated mining network; • ESS providers; and • Integrated mining networks. The procedure also encourages any controller or NSP not covered by the above to adopt AESCSF. Alinta Energy considers that a CPC Facility could have a material impact on the NWIS should a cyber event occur (depending on the configuration). Given this, consideration should be given to expanding the procedure to include a CPC Facility as a mandatory requirement rather than rely on the voluntary section 2.1 for this facility type.	Updated section 3.6 of the Procedure. If a CPC facility is a Critical Electricity Asset under the *Security of Critical Infrastructure Act 2018* (SOCI Act), it will be required to comply with the Cyber Security Procedure. If not, during the access and connection process, the ISO in consultation with the Host NSP and CPC facility will determine (depending on configuration) whether the CPC facility could have a material impact on the NWIS should a cyber security incident occur, and the applicability of the Cyber Security Procedure.
2.	2.7.4(a)	Alinta	Section 2.7.4(a) requires a NWIS Cyber Security Entity, by no later than 30 June each year, provide the ISO by email with a report in writing containing details of any Cyber Security Incident that has occurred in relation to, as the case may be, the relevant network, facility or ISO control desk (other than an incident report in accordance with section 2.8.1). Alinta Energy considers that this obligation simply adds additional compliance cost and regulatory burden for no demonstrated benefit. We recommend that the ISOCO sets out what it intends to do with this information and identifies the relative benefits from receiving this information. If there are no demonstrable benefits then Alinta Energy recommends that this obligation is removed.	Removed paragraph 2.7.4(a) New paragraph 3.8.4 of the Procedure to provide the purpose of collecting up to date Maturity Security Profile information. Updated paragraph 3.8.6 of the Procedure to clarify that this information will be treated as confidential information subject to Subchapter 11.2 of the Rules.

ISO INITIATED CHANGES – INTERIM CYBER SECURITY PROCEDURE V1.0

Item	Section	Initiated by	Comment	Change
1.	N/A	ISO	Standardisation across all of ISO's Procedures.	Updated wording, structure and formatting to standardise across all of ISO's Procedures.
2.	N/A	ISO	ISO's Interim Cyber Security Procedure was primarily concerned with the SOCI Act. Expanded the Procedure to cover Rule 103(1)(d) of the Rules for cyber-security requirements necessary to support its and Rules Participants' functions and activities under these Rules.	Updated the Procedure to include a new chapter 2 of the Procedure (Cyber Security Measurers) which outline the measures to be in place for the ISO, the ISO Control Desk and all Rules Participants.
3.	2.3	ISO	Rule 101 of the Rules requires that the Procedure developed under Rule 103 must set out measures for confidentiality and cyber security for visibility data. Rule 73(1) allows ISO to divide or combine or to create new Procedures; and to distribute matters between Procedures as it sees fit provided it follows the procedure change process in Appendix 2 of the Rues. Measures relating to the confidentiality and cyber security for visibility data are set out in the Visibility List Procedure, which can be found on the Pilbara ISOCo website www.pilbaraisoco.com.au.	Updated the Procedure to include new section 2.3 (Cyber Security for Visibility Data) to explicitly link the Cyber Security Procedure to the Visibility List Procedure.