Pilbara ISOCo
Independent System Operator

INTERIM CYBER SECURITY PROCEDURE

EFFECTIVE DATE: 28 JULY 2023

VERSION RELEASE HISTORY

Version	Effective Date	Changes	Approved
1.0	28 July 2023	Version 1 Published	James Campbell-Everden

Disclaimer

This document does not constitute legal advice or business advice and should not be relied on as a substitute for obtaining legal advice about the *Electricity Industry Act 2004* (WA), the Electricity Industry (Pilbara Networks) Regulations 2021, the Pilbara Networks Access Code, the Pilbara Networks Rules or any other applicable laws, procedures or policies.

While ISO has made every effort to ensure the quality of the information in this document, neither ISO, nor any of its employees, agents and consultants make any representation or warranty as to the accuracy, reliability, completeness, currency or suitability for particular purposes of that information.

To the maximum extent permitted by law, ISO and its advisers, consultants and other contributors to this document (or their respective associated companies, businesses, partners, directors, officers or employees) are not liable (whether by reason of negligence or otherwise) for any errors, omissions, defects or misrepresentations in this document, or for any loss or damage suffered by any persons who use or rely on the information in it.

TABLE OF CONTENTS

1. Introduction

1.1 Purpose and Scope

See Rule [103(1)(d)]

1.1.1 The purpose of this Procedure is to set out the matters necessary to support the ISO's and rules participants' functions and activities under the Pilbara Network Rules (Rules) in respect of Cyber Security Requirements under Rule 103(1)(d).

1.1.2 This Procedure is made in accordance with Sub-appendix 4.14 and 103(1)(d) of the Rules.

1.1.3 Other provisions of the Rules that support and apply to the making of this Procedure are those in Subchapter 3.6 {Procedures} and Subchapter 11.1 {Notices, publication and records}.

1.1.4 The *Electricity Industry Act 2004* (WA), the Electricity Industry (Pilbara Networks) Regulations 2021, the Pilbara Networks Access Code and Rules prevail over this Procedure to the extent of any inconsistency.

1.2 Definitions and Interpretation

1.2.1 Terms defined in the *Electricity Industry Act 2004* (WA), the Electricity Industry (Pilbara Networks) Regulations 2021, the Pilbara Networks Access Code and the Rules have the same meaning in this Procedure unless the context requires otherwise.

1.2.2 Where there is a discrepancy between the Rules and information on a term in this Procedure, the Rules take precedence.

1.2.3 The following principles of interpretation apply in this Procedure unless the context requires otherwise.

(a) Subchapter 1.2 of the Rules apply to this Procedure.

(b) References to time are references to Australian Western Standard Time.

(c) A reference to the Rules or Procedures made under the Rules, have the meaning given to them in the Rules.

(d) Words expressed in the singular include the plural and vice versa.

(e) A reference to a paragraph refers to a paragraph in the Procedure.

(f) A reference to a rule, subchapter or chapter refers to the relevant section in the Rules.

(g) References to the Rules in this Procedure in bold and square brackets, e.g. **"See Rule [XXX]"**, are included for convenience only, and do not form part of this Procedure.

(h) Any explanatory notes are included for context and explanation and do not form part of this Procedure.

(i) The Procedure prevails to the extent of any inconsistency with the explanatory notes contained within it.

1.2.4 Appendix A of this Procedure outlines the head of power rules that this Procedure is made under, as well as other obligations in the Rules covered by the Procedure.

1.2.5 For the purpose of this Procedure:

(a) **AESCSF** (Australian Energy Sector Cyber Security Framework) means the cyber security framework titled "2020-21 AESCSF Framework Core" published by AEMO for the Australian energy sector developed through collaboration by:

(i) the Australian Energy Market Operator (AEMO);

(ii) Department of Industry, Science, Energy and Resources (DISER);

(iii) Australian Cyber Security Centre (ACSC); and

(iv) The Department of Home Affairs (DHA),

as referred to in the SOCI Act (s30ANA(2)) and rules made under the SOCI Act

(b) **Critical Electricity Asset** has the meaning given in the SOCI Act, including any applicable rules made under that Act.

{Note: as at 1 July 2023, s10 of the SOCI Act stated:

(1) An asset is a Critical Electricity Asset if it is:

(a) network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules; or

(b) an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory, in accordance with subsection (2).

Note: The rules may prescribe that a specified Critical Electricity Asset is not a critical infrastructure asset (see section 9).

(2) For the purposes of paragraph (1)(b), the rules may prescribe requirements for an electricity generation station to be critical to ensuring the security and reliability of electricity networks or electricity systems in a particular State or Territory.}

(c) **Cyber Security Incident** has the meaning given in the SOCI Act

{Note: as at 1 July 2023, s12M of the SOCI Act states:

A Cyber Security Incident is one or more acts, events or circumstances involving any of the following:

(a) unauthorised access to:

(i) computer data; or

(ii) a computer program;

(b) unauthorised modification of:

(i) computer data; or

(ii) a computer program;

(c) unauthorised impairment of electronic communication to or from a computer;

(d) unauthorised impairment of the availability, reliability, security or operation of:

(i) a computer; or

(ii) computer data; or

(iii) a computer program.}

(d) **Cyber Security Requirements** means the requirements set out in section 2 of this Procedure.

(e) **NWIS Cyber Security Entity** means the person identified under section 2.3, 2.4, 2.5 or 2.5 of this Procedure that is responsible for complying with the Cyber Security Requirements in respect of a network or facility.

(f) **Responsible Entity** means the person responsible for a Critical Electricity Asset in accordance with s(10) of the SOCI Act

{Note: as at 1 July 2023, s12L(10) of the SOCI Act states:

"(10) The Responsible Entity for a Critical Electricity Asset is:

(a) the entity that holds the licence, approval or authorisation (however described) to operate the asset to provide the service to be delivered by the asset; or

(b) if another entity is prescribed by the rules in relation to the asset—that other entity." }

(g) **Relevant Impact** means a Relevant Impact of a Cyber Security Incident on a critical infrastructure asset as described in the SOCI Act, read as if references to a critical infrastructure asset were references to the network, facility, ISO control desk or other equipment in respect of which a person is the NWIS Cyber Security Entity.

{Note: as at 1 July 2023, s8G(2) of the SOCI Act states:

"(2) Each of the following is a ***Relevant Impact*** of a Cyber Security Incident on a critical infrastructure asset:

(a) the impact (whether direct or indirect) of the incident on the availability of the asset;

(b) the impact (whether direct or indirect) of the incident on the integrity of the asset;

(c) the impact (whether direct or indirect) of the incident on the reliability of the asset;

(d) the impact (whether direct or indirect) of the incident on the confidentiality of:

(i) information about the asset; or

(ii) if information is stored in the asset—the information; or

(iii) if the asset is computer data—the computer data." }

(h) **Risk Management Program** means a critical infrastructure Risk Management Program as defined in the SOCI Act.

{Note: as at 1 July 2023, s30AH(1) of the SOCI Act states:

"(1) A ***critical infrastructure risk management program*** is a written program:

(a) that applies to a particular entity that is the Responsible Entity for one or more critical infrastructure assets; and

(b) the purpose of which is to do the following for each of those assets:

(i) identify each hazard where there is a material risk that the occurrence of the hazard could have a Relevant Impact on the asset;

(ii) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;

(iii) so far as it is reasonably practicable to do so—mitigate the Relevant Impact of such a hazard on the asset; and

(c) that complies with such requirements (if any) as are specified in the rules."}

(i) **SOCI Act** means the *Security of Critical Infrastructure Act 2018* (Cth)

(j) **Target State Maturity Security Profile** means a measure of target state maturity in accordance with the AESCSF of SP-1, SP-2 or SP-3.

{Note: the AESCSF Framework Overview published by AEMO contains a description of security profiles, their relationship with maturity indicator levels, target state maturity and other related information.]}

2. Cyber security

2.1 AESCSF adoption encouraged

2.1.1 Any controller or NSP that does not need to comply with the requirements of the remainder of section 2 of this Procedure is encouraged to make use of the AESCSF by, for example:

(a) undertaking an assessment in accordance with the AESCSF of any of its network or facilities that are connected to the NWIS;

(b) develop a Risk Management Program in relation to any Relevant Impact of a hazard that may occur in relation to the network or facility; and

(c) develop a program or roadmap to increase, over time, its Target State Maturity Security Profile level in relation to the asset.

2.2 Covered networks and ISO control desk

See Rule [45]

2.2.1 While delegated ISO real-time control desk functions under Rule 45, the Regional Power Corporation (Horizon Power) is the NWIS Cyber Security Entity for the ISO control desk.

2.2.2 If a covered network is a Critical Electricity Asset, the Responsible Entity for that asset is the NWIS Cyber Security Entity for the covered network.

2.2.3 If a covered network is not a Critical Electricity Asset, the registered NSP of the covered network is the NWIS Cyber Security Entity for the covered network.

2.2.4 A NWIS Cyber Security Entity for a covered network or the ISO control desk must:

(a) achieve and maintain a Target State Maturity Security Profile of not less than SP-1 (Security Profile 1) in respect of that covered network by 18 August 2024; and

(b) comply with the requirements of sections 2.7 and 2.8 of this Procedure.

2.3 Registered NSPs

See Rule [Subchapter 4.1]

2.3.1 This section 2.3 applies to any non-covered NWIS network that is not an excluded network or an integrated mining network in respect of which a person is the registered NSP in accordance with Rules Subchapter 4.1.

2.3.2 If a non-covered network to which this section 2.3 applies is a Critical Electricity Asset, the Responsible Entity for that Critical Electricity Asset is the NWIS Cyber Security Entity for the non-covered network.

2.3.3 If a non-covered network to which this section 2.3 applies is not a Critical Electricity Asset, registered NSP of the non-covered network is the NWIS Cyber Security Entity in respect of the non-covered network.

2.3.4 A NWIS Cyber Security Entity for a non-covered network to which this section 2.3 applies must:

(a) achieve and maintain a Target State Maturity Security Profile of not less than SP-1 (Security Profile 1) in respect of that non-covered network by 18 August 2024; and

(b) comply with the requirements of sections 2.7 and 2.8 of this Procedure.

2.4 ESS providers

2.4.1 If a facility used to provide an essential system service is a Critical Electricity Asset, the Responsible Entity for the asset is the NWIS Cyber Security Entity in respect of the facility.

2.4.2 If a facility used to provide an essential system service is not a Critical Electricity Asset, the controller of the facility is the NWIS Cyber Security Entity in respect of the facility.

2.4.3 A NWIS Cyber Security Entity in respect of a facility used to provide an essential system service, must:

(a) achieve and maintain a Target State Maturity Security Profile of not less than SP-1 (Security Profile 1) or its reasonable equivalent in respect of that facility by no later than 18 August 2024; and

(b) comply with the requirements of sections 2.7 and 2.8 of this Procedure.

2.5 Integrated mining network

See Rule [5]

2.5.1 If a facility located in an integrated mining network is a Critical Electricity Asset, the Responsible Entity for that asset is NWIS Cyber Security Entity in respect of the facility.

2.5.2 If a facility located in an integrated mining network is not a Critical Electricity Asset, the controller of the facility used to provide the essential system service is the NWIS Cyber Security Entity in respect of the facility.

2.5.3 A person who is NWIS Cyber Security Entity in accordance with section 0 or section 2.5.2 must:

(a) achieve and maintain a Target State Maturity Security Profile of not less than SP-1 (Security Profile 1) or its reasonable equivalent in respect by no later than 18 August 2024; and

(b) comply with sections 2.7 and 2.8 of this Procedure.

2.6 Concurrent obligations

See Rule [292(1)]

2.6.1 A person may be a NWIS Cyber Security Entity in accordance with more than one of sections 2.2 to 2.5.

2.6.2 A person who is a NWIS Cyber Security Entity under more than one of sections 2.2 to 2.5:

(a) is to comply with this procedure once in relation to any particular network or facility; and

(b) the person may combine any information or report to be prepared or provided in accordance with sections 2.7 and 2.8 or this Procedure more generally into a single instrument or report: see Rule 292(1).

2.7 Reporting obligations

2.7.1 Subject to section 2.7.2, a NWIS Cyber Security Entity must, as soon as practicable after the commencement of this Procedure, advise the ISO:

(a) whether it is a Responsible Entity for critical electricity infrastructure under the SOCI Act that is located in the NWIS;

(b) if it has identified a Target State Maturity Security Profile under the AESCSF is in respect of the network, facility or other equipment for which it is the NWIS Cyber Security Entity and, if so, what that Target State Maturity Security Profile level is; and

(c) if it has not identified a Target State Maturity Security Profile level under the AESCSF in respect of the network, equipment or facility for which it is the NWIS Cyber Security Entity, when it expects to do so.

2.7.2 For the purposes of sections 2.7.1(b) and sections (c), a NWIS Cyber Security Entity for an integrated mining network or facility forming part of an integrated mining system is to advise the ISO if it has a maturity level reasonably equivalent to a Target State Maturity Security Profile under the AESCSF, if so, what that reasonably equivalent maturity level is and, if not, if and when it expects to do so.

2.7.3 A NWIS Cyber Security Entity that is a Responsible Entity for critical electricity infrastructure of the kind described in clause sections 2.2 to 2.5 of this procedure must advise the ISO if it is required to comply with Part 2A {Critical infrastructure Risk Management Programs} of the SOCI Act and corresponding rules made under that Act.

2.7.4 By no later than 30 June each year, a NWIS Cyber Security Entity must provide the ISO by email with a report in writing containing the following information:

(a) 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);

(b) the current Target State Maturity Security Profile level achieved by the NWIS Cyber Security Entity in respect of the relevant network and or facility (as the case may be);

(c) whether the NWIS Cyber Security Entity has maintained the Target State Maturity Level Security Profile in respect of the relevant network or facility (as the case may be) identified in the previous report provided to the ISO under sections 2.7.1, 2.7.2(a) or this section 2.7.4(c) as applicable; and

(d) Whether the NWIS Cyber Security Entity intends to increase its Target State Maturity Security Profile level in the following 12 to 24 months.

2.8 Cyber Security Incidents

2.8.1 A NWIS Cyber Security Entity who becomes aware that a Cyber Security Incident is occurring and is having a Relevant Impact on, as the case may be, the network, facility or the ISO control desk, must:

(a) so far as practicable, within 12 hours of becoming aware of the occurrence of the incident, notify the ISO and the ISO control desk whether, in the reasonable opinion of the NWIS Cyber Security Entity:

(i) the Cyber Security Incident may or is likely to have material adverse implications for the reliability, safety of the NWIS; and

(ii) a system coordination meeting should be convened to consider the Cyber Security Incident and determine what measures, if any, are to be taken in response;

(b) so far as practicable, within 7 days, provide the ISO by email with a report in writing about the incident that includes a general description of its nature and character, the extent of its impact and, if known, its anticipated duration;

(c) while the Cyber Security Incident persists, keep the ISO informed and updated in respect of the matters referred to in sections 2.8.1(a) and 2.8.1(b)(b); and

(d) notify the ISO and the ISO control desk when the Cyber Security Incident has ceased.

Appendix A: Relevant Rules

Table 1 details the Rules under which this Procedure has been developed and where an obligation, process or requirement has been documented in this Procedure.

Table 1: Relevant rules

Pilbara Networks Rules
5
45
Subchapter 3.6
Subchapter 4.1
103(1)(d)
Subchapter 11.1
292
Sub-appendix 4.14