

DRAFT DECISION:

**REVIEW OF SUBCHAPTER 7.3 AND 7.4 OF THE PILBARA
NETWORKS RULES**

4 OCTOBER 2024

TABLE OF CONTENTS

TABLE OF DRAFT ECOMMENDATIONS	4
ANNOTATED TABLE OF ISSUES FROM ISSUES PAPER.....	6
1. INTRODUCTION.....	10
1.1 PURPOSE OF THIS REVIEW	10
1.2 THE LEGISLATIVE FRAMEWORK	11
1.3 EPWA’S PNR EVOLUTION REVIEW	11
1.4 REFERENCES IN THIS DRAFT DECISION TO “OUTAGES” GENERALLY INCLUDES ALL NOTIFIABLE EVENTS.....	12
2. CONSULTATION PROCESS AND TIMELINE	13
2.2 FIRST ROUND OF CONSULTATION (COMPLETED) – INFORMAL FEEDBACK	13
2.3 SECOND ROUND OF CONSULTATION (NOW) – WRITTEN SUBMISSIONS AND COMMENTS	14
2.4 CONFIDENTIALITY AND TRANSPARENCY	14
2.5 FURTHER INFORMATION	14
3. CASE STUDIES	15
3.1 ABOUT THESE CASE STUDIES	15
3.2 CASE STUDY 1: EXTENDED INTERCONNECTOR OUTAGE EXPOSES REGION TO CONTINGENT ISLANDING RISK	15
3.3 CASE STUDY 2: TRANSMISSION OUTAGE CREATING RISK FOR ANOTHER RETAILER’S CUSTOMERS	16
3.4 CASE STUDY 3: UNSCHEDULED GENERATOR UNAVAILABILITY.....	17
3.5 CASE STUDY 4: OUTAGE OF A POWER STATION’S ANCILLARY EQUIPMENT.....	18
4. STRUCTURAL MATTERS	21
4.1 INTRODUCTION.....	21
4.2 VERTICAL INTEGRATION.....	21
4.3 TRANSPARENCY.....	23
5. DEFINITIONS	25
5.1 “OUTAGE” AND “NOTIFIABLE EVENT”	25
5.2 “SYSTEM COORDINATION MATTERS”.....	26
5.3 SYSTEM STATES	27
5.4 “ISLAND”	27
DRAFT DECISION – REVIEW OF SUBCHAPTER 7.3 AND 7.4 OF THE PNR	1

6.	OBJECTIVES, FUNCTIONS AND POWERS	28
6.1	PRIORITISING SYSTEM SECURITY	28
6.2	CLEAR ROLE FOR THE ISO TO ASSESS, COORDINATE AND OVERSEE MANAGEMENT OF NOTIFIABLE EVENTS.....	29
6.3	RE-FOCUSSED ROLE FOR THE ISO CONTROL DESK	31
6.4	STANDARDISED RISK ASSESSMENT	31
6.5	ADEQUATE POWERS TO INTERVENE	32
6.6	AN OUTAGE MANAGEMENT PROCEDURE.....	32
7.	THE OUTAGE PLANNING AND ASSESSMENT PROCESS	34
7.1	THE CURRENT PROCESS	34
7.2	OUTAGE MANAGEMENT UNDER OTHER REGIMES.....	36
7.3	RECOMMENDED PROCESS FOR PILBARA	42
7.4	HOW THE SECTION 7.3 PROCESS MIGHT BE IMPLEMENTED.....	49
7.5	HOW THE SECTION 7.3 PROCESS WOULD HAVE DEALT WITH THE FOUR CASE STUDIES IN SECTION 3	49
8.	MITIGATION OF OUTAGES	51
8.1	INTRODUCTION.....	51
8.2	WHO DETERMINES WHICH MITIGATIONS SHOULD BE IMPLEMENTED?	51
8.3	WHO IS RESPONSIBLE FOR IMPLEMENTING MITIGATIONS?	52
8.4	DEALING WITH THE COSTS OF MITIGATION	52
8.5	USE OF ESS TO MITIGATE OUTAGES	53
9.	MATTERS LEFT FOR A BROADER REVIEW	57
	APPENDIX 1: STAKEHOLDER FEEDBACK ON ISSUES PAPER.....	58
	APPENDIX 2: RELEVANT RULES	66
8	GLOSSARY	66
162	THE SYSTEM SECURITY OBJECTIVE.....	66
163	DEFINITION OF INSIDE THE TECHNICAL ENVELOPE	67
164	DEFINITION OF SECURE STATE	67
165	DEFINITION OF NORMAL OPERATING CONDITIONS	67
166	DEFINITION OF NOTIFIABLE EVENT	68
167	DEFINITION OF SYSTEM COORDINATION MATTERS	68
173	OBJECTIVES OF THIS SUBCHAPTER 7.3 AND SUBCHAPTER 7.4.....	69
	DRAFT DECISION – REVIEW OF SUBCHAPTER 7.3 AND 7.4 OF THE PNR	2

174	SYSTEM COORDINATION MEETINGS	69
175	ACTIVITIES BETWEEN SYSTEM COORDINATION MEETINGS	70
176	SYSTEM COORDINATION MEETINGS AND DISCUSSIONS – CONFIDENTIAL INFORMATION ...	70
177	ISO TO PRODUCE SYSTEM COORDINATION REPORT	70
178	REVIEW OF THIS SUBCHAPTER 7.3 AND SUBCHAPTER 7.4	71
179	IF A NEAR-TERM EVENT ARISES BETWEEN SYSTEM COORDINATION MEETINGS	71
180	NOTIFICATION OBLIGATIONS	71
181	OUTAGES OF FACILITIES	72
182	RESOLVING SCHEDULING CONFLICTS	72
183	OBLIGATIONS TO REPORT CONTINGENCIES AND UNPLANNED EVENTS	72
 APPENDIX 3: WEM OUTAGE PROCESS.....		74

TABLE OF DRAFT RECOMMENDATIONS

		page
Draft Recommendation 1	That although Subchapters 7.3 and 7.4 should leave room for informal cooperation and collaboration between market participants, they should not require it.	22
Draft Recommendation 2	That wherever possible, information about notifiable events should be publicly available. That in designing the detail of these rules, consideration should be given to whether any of this information needs to be kept confidential, and if so how transparency is nonetheless to be maximised.	24
Draft Recommendation 3	That Subchapters 7.3 and 7.4 should enable the processes for notification, assessment, approval, scheduling and management of notifiable events to differentiate between and integrate across the various types of such events as appropriate, including: <ul style="list-style-type: none"> • planned maintenance and routine upgrades; • major or extended outages; • commissioning and testing; • events in integrated mining networks; • events in the Pluto facility; and • events in any other connection point compliance facility. 	26
Draft Recommendation 4	That the PNR and Procedures should seek to minimise any risk of ambiguity, inconsistency or gaps arising from the potential overlap between: <ul style="list-style-type: none"> • notifiable events being managed under Subchapters 7.3 and 7.4; • contingencies and pre-contingent threats being managed under Subchapter 7.5 and the Protocol Framework; and • the procurement and activation of ESS under Chapter 8. 	26
Draft Recommendation 5	That the PNR's and Procedures' references to "outage" and "notifiable event" be made consistent.	26
Draft Recommendation 6	That the changes implemented under Draft Recommendations 3, 4 and 5 ensure that the limitations of the definition of "island" do not constrain the circumstances in which mitigation measures for notifiable events are considered or implemented.	27
Draft Recommendation 7	That the primary objective for Subchapters 7.3 and 7.4 be revised, to focus solely on achieving the system security objective.	29
Draft Recommendation 8	That the ISO be given the overarching function of managing and approving notifiable events, including supervising their notification and scheduling, assessing their risks, and supervising, and as necessary directing, the management (including mitigation) of those risks.	30
Draft Recommendation 9	That the ISO develop its own resources to deliver the function described in Draft Recommendation 8.	30

Draft Recommendation 10	That the ISO control desk's functions be restricted to real-time operations, contingency response and managing near-term pre-contingent threats such as cyclones and bushfires.	31
Draft Recommendation 11	That the rules or a procedure require the ISO to develop a standardised risk assessment framework for assessment, approval, scheduling and management of notifiable events, and require all participants to use that framework.	32
Draft Recommendation 12	That the rules and procedures give the ISO the necessary powers to give directions in connection with the scheduling and management of notifiable events. That this include a power to approve or disapprove notifiable events with or without conditions, and a power to recall equipment where appropriate.	32
Draft Recommendation 13	That the ISO develop a new Procedure to govern the notification, assessment, approval, scheduling and management of notifiable events.	32
Draft Recommendation 14	That a notifiable event management process be established for the NWIS as described in this section 7.3.	42
Draft Recommendation 15	The ISO, through its power to approve or reject proposals for notifiable events, will be responsible for determining which mitigations or other management measures should be implemented for an event.	50
Draft Recommendation 16	That the ISO be empowered to direct the proponent, and if appropriate other participants, to take measures to mitigate notifiable events. That the ISO control desk have the power to activate these measures as necessary during real-time operations.	51
Draft Recommendation 17	That a broader review address the question of how notifiable event mitigation costs should be identified, assessed and allocated.	52
Draft Recommendation 18	That during the detailed design of the new regime, consideration be given to whether the ISO should be permitted to utilise ESS contracts to manage notifiable events, and if so in what circumstances. Further, if so, that the review under Draft Recommendation 17 determine how the resulting ESS costs should be allocated.	54
Draft Recommendation 19	That the ISO propose urgent rule and procedure changes as necessary, to enable it to use ESS to mitigate notifiable events, as an interim solution pending any more complete rule changes which may be developed following this review and any broader review. Further, that pending a suitable answer to the question of how mitigation costs should be identified, assessed and allocated, the costs of ESS contracts used in this fashion should be recovered through standard Subchapter 8.3 processes.	55
Draft Recommendation 20	That in due course a broader review should address the matters identified in this section 9.	56

ANNOTATED TABLE OF ISSUES FROM ISSUES PAPER

The first two columns in following table are reproduced from the Issues Paper dated 19 July 2024. The final column shows how this Draft Decision proposes that the issue be addressed.

Issue (as expressed in Issues Paper)	Recommended treatment
<p>Issue 1 Subchapters 7.3 and 7.4 do not specify the “system security objective” as their primary objective.</p>	<p>The ISO proposes that this be remedied. See Draft Recommendation 7.</p>
<p>Issue 2 The emphasis on informality and collaboration has resulted in processes under Subchapters 7.3 and 7.4 that lack rigour. It has been suggested that the Pilbara outage management regime should copy the WEM Rules’.</p>	<p>The ISO proposes a new outage management procedure which is less complex than the WEM regime, but which provides more formal communication, greater transparency and less reliance merely on collaboration.</p> <p>For the new process, see Draft Recommendation 14 and section 7.3.</p> <p>For transparency, see Draft Recommendation 2.</p> <p>For reduced reliance on merely collaboration, see Draft Recommendations 1 and 8, and other draft recommendations discussed in the following rows of this table.</p>
<p>Issue 3 The definition of “notifiable event” is very broad. The Subchapter 7.3 and 7.4 processes may need to differentiate between, and integrate across, different classes of notifiable event, for example:</p> <ul style="list-style-type: none"> • planned maintenance and routine upgrades; • major or extended outages; • commissioning and testing; • events in integrated mining networks; • events in the Pluto facility; and • events in another connection point compliance facility. 	<p>The ISO proposes that the definition be left as is, but that the Subchapter 7.3 and 7.4 processes differentiate and integrate as appropriate between the different classes of event. See Draft Recommendation 3.</p>
<p>Issue 4 Under the current rules, a planned outage is a contingency, and not a pre-contingent threat, and so falls to be managed under rule 187 which has a focus on reactive post-contingent responses.</p>	<p>Generally left to a broader review, but the new rules and procedures recommended in this draft decision will address this ambiguity. See Draft Recommendation 4.</p> <p>Draft Recommendation 10 proposes that the ISO control desk’s functions be restricted to real-time and near real-time matters.</p>
<p>Issue 5 Because a planned outage is a contingency, whenever a planned outage is occurring anywhere in the NWIS, the system is defined to be “outside normal operating conditions”, enabling relevant protocols to be activated (if their activation conditions are met)—but the pre-contingent protocol will not be available. The ISO seeks stakeholder feedback on whether this is a desirable outcome, or whether:</p> <p>(a) planned outages would be better managed as a variety of pre-contingent threat; or</p> <p>(b) the definition of “normal operating state” should be changed so that the system can (or</p>	<p>Left to a broader review.</p>

	<p>can sometimes) remain in this state despite planned outages being under way; or</p> <p>(c) a fourth operating state is required, specifically to deal with planned outages.</p>	
Issue 6	<p>The rules rely primarily on oral discussion as the means for NSPs to notify the ISO and other NSPs of notifiable events. This minimises the compliance burden for near-term coordination, but may not be the optimum way to manage scheduling and assessment (including modelling) for outages which are known well in advance.</p>	<p>The ISO proposes a new outage management procedure with more formal communication, see section 7.3 and Draft Recommendation 14.</p> <p>For transparency, see Draft Recommendation 2.</p>
Issue 7	<p>There is no Procedure regarding outage management and the rules do not provide for one.</p>	<p>The ISO proposes that this be remedied. See Draft Recommendation 13.</p>
Issue 8	<p>The rules regarding the composition, agenda and duration of system coordination meetings are too prescriptive. These matters may be better located in a Procedure.</p>	<p>This will be addressed in the changes described under Issues 2, 6 and 7 above. The focus will shift from the system coordination meeting to the approval process described in section 7.3.</p>
Issue 9	<p>The rules do not clearly allocate responsibility for determining the impacts a notifiable event might have on the power system, including security, reliability, constraints and ESS, or for the risk and other analysis and modelling required to assess these things, and do not provide a mechanism for accommodating different risk appetites or resolving disagreements on these matters.</p>	<p>The ISO proposes that the ISO be given this function. See Draft Recommendation 8.</p>
Issue 10	<p>If there is disagreement between Horizon Power and another NSP regarding the assessment of a notifiable event, the ISO's use of ISO control desk staff to help in the assessment places a focus on how Horizon Power manages the staff's conflict of interest.</p>	<p>The ISO proposes that the ISO control desk's role be restricted to real-time and near real-time matters. See Draft Recommendation 10.</p> <p>Outage management will be an ISO (not ISO control desk) function. See Draft Recommendation 8 and the process described in section 7.3.</p>
Issue 11	<p>There is no general requirement for planned outages and other notifiable events to be approved.</p>	<p>See the proposed new outage management procedure in section 7.3. See Draft Recommendation 14.</p>
Issue 12	<p>Except in the case of a scheduling conflict, the rules do not provide for a notifiable event to be stopped or deferred, or otherwise be the subject of a direction, pending satisfactory resolution of any disagreement regarding its impacts on other participants, e.g. by way of its impact on security, reliability, constraints or ESS.</p>	<p>See the proposed new outage management procedure in section 7.3. See Draft Recommendation 14.</p> <p>The ISO will administer this, see Draft Recommendation 8.</p>
Issue 13	<p>The definition of scheduling conflict is limited to events which may take the system outside the technical envelope or otherwise pose an unacceptable risk to security or reliability. This does not require the system to be maintained in a secure state, and does not assess other impacts such as on risk, constraints, ESS or cost.</p>	<p>This will be addressed by:</p> <ul style="list-style-type: none"> • the new focus on the system security objective, see Draft Recommendation 7; • the proposed new outage management procedure in section 7.3, see Draft Recommendation 14; and

		<ul style="list-style-type: none"> the ISO being given the function of managing notifiable events, see Draft Recommendation 8.
Issue 14	The ISO's power to intervene in a scheduling conflict is not enlivened until it has first determined that a consensus is unlikely to be reached in time. This could create system risk.	The ISO proposes that it be given a general power to approve notifiable events, assess risk and direct mitigations. See Draft Recommendation 8.
Issue 15	Are the ISO's direction powers under rules 182(3) to (5) appropriate and sufficient?	<p>The proposed new outage management procedure in section 7.3, see Draft Recommendation 14, should ensure that most mitigations have been established by the time the outage proposal is approved, see Draft Recommendations 12.</p> <p>But the ISO proposes that it also have a general power to direct mitigations, see Draft Recommendation 16.</p>
Issue 16	The rules do not deal with how network planning criteria are to be dealt with in assessing, managing and mitigating notifiable events.	<p>The proposed new outage management procedure in section 7.3 (see Draft Recommendation 14), applying a standardised risk assessment framework (see Draft Recommendation 11), will take network planning criteria into account.</p> <p>The broader question of how the PNR deal with network planning criteria is a matter for a broader review.</p>
Issue 17	The rules and protocols do not deal cleanly with a situation in which islanding has not yet occurred but pre-contingent actions are necessary, e.g. to prevent islanding or ensure the island is secure (or at least inside the technical envelope) should islanding occur.	<p>The ISO proposes that the new regime work around this deficiency. See Draft Recommendation 6.</p> <p>Otherwise this is a matter for a broader review.</p>
Issue 18	There is no clear mechanism for identifying the measures necessary to manage or mitigate a notifiable event, and no clear obligation on any person to implement those measures once identified.	<p>This will be addressed by the proposed new outage management procedure in section 7.3, see Draft Recommendation 14, and also by the proposal that there be a standardised risk assessment framework, see Draft Recommendation 11.</p> <p>The ISO's direction powers will ensure the risks are managed, see Draft Recommendations 12 and 16.</p>
Issue 19	There is no practicable mechanism to resolve differences of opinion in connection with notifiable events, for example regarding risk assessment and how or by whom a notifiable event is to be mitigated or managed.	This will be the ISO's function, see Draft Recommendation 8, under the proposed new outage management procedure in section 7.3, see Draft Recommendation 14.
Issue 20	A question has been raised as to whether there should be any exemption from rules participants' system security obligations during a notifiable event.	The ISO does not consider this appropriate.
Issue 21	The rules do not deal separately with the specification and procurement of, and cost recovery for, additional ESS, or machine start or other services, when this is required to manage or mitigate a notifiable event, rather than as part of normal system operations under Chapter 8.	<p>The ISO proposes that the new regime work around this deficiency. See Draft Recommendation 4.</p> <p>For the use of ESS to mitigate outages, see section 8.5 and Draft Recommendations 18 and 19.</p>

		Otherwise, the possible overlaps between Subchapters 7.3, 7.4, 7.5 and Chapter 8 are a matter for a broader review. See Draft Recommendation 20.
Issue 22	The ISO has no power to direct how a notifiable event is to be managed or mitigated.	The ISO proposes that this be remedied. See Draft Recommendations 12, 15 and 16.
Issue 23	The nature and timing of pre-contingent powers required to manage notifiable events are likely sufficiently different to the post-contingent powers the ISO control desk needs to manage contingencies, that it is appropriate for them to be exercised by the ISO rather than the ISO control desk. The current pre-contingent protocol was not designed to manage notifiable events.	The ISO proposes that the ISO control desk's role be restricted to real-time and near real-time events, see Draft Recommendation 10. The management of notifiable events will thus fall to the ISO, not the ISO control desk, under the ISO's new functions and powers described above. Specifically, this will be the ISO's function (see Draft Recommendation 8) and it will have the necessary powers (see Draft Recommendations 12, 15 and 16).
Issue 24	The rules lack any mechanism to determine and apportion the costs of managing and mitigating notifiable events. A choice needs to be made as to whether mitigation costs should be apportioned on a causer pays, beneficiary pays or socialised basis, or some combination of these or some other basis.	Because this raises material issues of policy, this should be addressed by a broader review. See Draft Recommendation 17. However, as an interim measure for the use of ESS to mitigate outages and recover the costs of doing so, see section 8.5 and Draft Recommendations 18 and 19.
Issue 25	The regime for notifying, assessing, managing and mitigating notifiable events must appropriately balance transparency, accountability, confidentiality and competition.	The ISO proposes that the regime lean towards transparency wherever possible, See Draft Recommendation 2.
Issue 26	If the ISO is given an expanded role to address the issues identified in this paper, it would have resourcing and hence cost implications.	See Draft Recommendation 9.

1. Introduction

1.1 Purpose of this review

- 1.1.1 A primary goal of the Pilbara regime¹ is to maintain and improve power system security.² Chapter 7 of the Rules deals with the main operational aspects of this, and one important component of Chapter 7 is the processes set out in Subchapters 7.3 and 7.4 for notifying, assessing, coordinating and managing planned and unplanned outages and other “notifiable events”.³
- 1.1.2 Rule 178 requires the ISO periodically to conduct a review of Subchapter 7.3 and 7.4’s processes against the “Pilbara electricity objective”.⁴ Having had a chance to observe the current processes in operation for 3 years, and especially given the ISO’s experience administering and observing them over the last roughly 12 months (see Case Studies in section 3 below), the ISO considered that it was time to undertake this review.
- 1.1.3 The NWIS supports some of Australia’s biggest exporters and two of the biggest bulk export ports in the world. Even today, the economic cost of disruptions in electricity supply can be very large. But the Pilbara electricity market is about to evolve and expand. Across the region consumers are embarking on major decarbonization and electrification programs. These will require a significant expansion of the grid and the connection of numerous new renewable generators. Not only will this make power system security and reliability even more important than it is today, but also the works required for the expansion will involve much more commissioning, testing and transmission tie-ins than have occurred in the past. The NWIS’s outage management processes must be able to adequately assess and manage the associated risks.
- 1.1.4 On 19 July 2024 the ISO published an **Issues Paper**. Since then it has met with stakeholders and received informal submissions, and is now in a position to publish this Draft Decision.
- 1.1.5 The ISO seeks feedback from stakeholders on this Draft Decision, or otherwise on the Subchapter 7.3 and 7.4 processes.

¹ Implemented under Part 8A of the *Electricity Industry Act 2004*, and including the *Electricity Industry (Pilbara Networks) Regulations 2021*, the *Pilbara Networks Access Code*, *Pilbara Networks Rules*, *Harmonised Technical Rules* and various procedures made under the Rules.

² *Electricity Industry Act 2004* sections 119(1)(c), 119(2), 120K(1) and (2), and 120W(4)(a)

³ 119(2) A “notifiable event” is any planned or anticipated outage or other system event which might credibly be expected to adversely effect power system security, the delivery and effectiveness of essential system services, or the ability of covered transmission NSPs to provide contracted access services: Rule 166.

⁴ Section 119(2) of the *Electricity Industry Act 2004* sets out the Pilbara electricity objective:

“... to promote efficient investment in, and efficient operation and use of, services of Pilbara networks for the long-term interests of consumers of electricity in the Pilbara region in relation to —
(a) price, quality, safety, reliability and security of supply of electricity; and
(b) the reliability, safety and security of any interconnected Pilbara system.”

1.2 The legislative framework

IMPORTANT NOTICE: For readability, this paper generally gives simplified narrative descriptions of Rules and other instruments. Please refer to the published Rules and Procedures for the exact wording.

- 1.2.1 Part 8A of the *Electricity Industry Act 2004* provides the statutory basis of the Pilbara regime, and sets out the Pilbara electricity objective and the ISO's core functions, which include maintaining and improving power system security in the NWIS.⁵
- 1.2.2 Part 8A of the Act empowers regulations (the *Electricity Industry (Pilbara Networks) Regulations 2021*) which in turn empower the making of rules including the *Pilbara Networks Rules*.
- 1.2.3 The *Pilbara Networks Rules* empower the ISO and others to make *Procedures* to supplement the Rules including, importantly, the *Protocol Framework Procedure* which sets out the *Protocols* by which the ISO Control Desk and NSPs are to manage contingency events and other matters which may threaten power system security.
- 1.2.4 Section 3 of the Issues Paper summarizes the Pilbara regime's design philosophy, which emphasizes self-determination for, and collaboration between, the three registered NSPs.

1.3 EPWA's PNR Evolution review

- 1.3.1 During this review, matters have arisen which affect the PNR more broadly than just Subchapters 7.3 and 7.4, and so should be considered in due course as part of a broader review. This draft decision identifies such matters without attempting to resolve them. They are listed in section 9.
- 1.3.2 As part of its *Evolving the Pilbara Networks Rules (PNR Evolution)* project, EPWA is undertaking a wide-ranging review of the Pilbara regime's governance and the PNR generally. This is being progressed with the Pilbara Advisory Committee,⁶ and EPWA's current reform priorities are summarised in **Figure 1**:⁷

⁵ *Electricity Industry Act 2004*, section 120W(4)(a).

⁶ See Pilbara Advisory Committee meeting papers and minutes for 2024 (available [here](#)).

⁷ See Pilbara Advisory Committee meeting papers for 29 August 2024 2024 (available [here](#)), pdf page 34.

Prioritised initiatives to focus on in advance of the consultation paper?

<p>Power system security and reliability</p> <ul style="list-style-type: none"> Reliability standard and supply adequacy Long term planning Outage planning ESS definitions and procurement ESS cost allocation Responsibility for setting system strength requirements 	<p>Terminology</p> <ul style="list-style-type: none"> Registration constructs – definition of “NSP” Definition and use of “energisation” and “commercial operations” Consistency between PNR and HTR
<p>Scheduling, dispatch and settlement</p> <ul style="list-style-type: none"> Balancing service with (optional) reduced load following requirements Metering obligations Load shedding arrangements Fee allocation 	<p>Governance of the ISO</p> <ul style="list-style-type: none"> Board composition Resourcing and budget Ringfencing and confidentiality regime
<p>New connections</p> <ul style="list-style-type: none"> NSP to NSP connection arrangements, including constrained access Process for new transmission build, including transmission pricing and constrained access Registration category and requirements for storage facilities Registration category and requirements for DSR Exemptions and derogations from the HTR 	<p>Compliance and enforcement</p> <ul style="list-style-type: none"> Responsibilities and process for compliance monitoring Enforcement options
<p>Working together for a brighter energy future.</p>	

Legend
Tier 1 (2+ criteria)
Tier 2 (1 criteria)
Progressing elsewhere

Does the PAC have any comments on the initiative list, or the priority initiatives?

Figure 1 – EPWA’s PNR Evolution review priorities

1.3.3 There is clearly some overlap between the issues addressed by this rule 178 review and EPWA’s review, although the EPWA review will be broader. The ISO will leave it to EPWA to decide whether a matter listed in section 9 should be addressed in its PNR Evolution review.

1.3.4 **The ISO does not propose to share with EPWA the confidential and informal submissions it has received to date regarding this review.** Therefore, where a stakeholder has submitted to the ISO on a matter which this draft decision indicates is deferred to a broader review, the stakeholder should ensure it communicates its views to EPWA at the appropriate time.

1.4 References in this draft decision to “outages” generally includes all notifiable events

1.4.1 The PNR recognise that the range of things which may need to be notified, assessed, coordinated and managed under Subchapters 7.3 and 7.4 will sometimes be broader than just “outages”. The PNR uses the expression “**notifiable events**” to describe this wider category. As discussed in section 4.3.6, the ISO does not propose any change to this language.

1.4.2 But because it represents the most common class of notifiable event and matches common usage, for ease of reading this draft decision generally uses the shorter expression “outage” without intending by doing so to narrow the discussion’s scope. Except where the distinction is drawn explicitly, **you should read references in this document to “outages” as including all “notifiable events”, including commissioning and testing.**

1.4.3 Reminders of this are placed near the beginning of each chapter.

2. Consultation Process and Timeline

- 2.1.1 Under rule 178, as part of this review the ISO is required to consult with registered NSPs, registered controllers and undertake public consultation following the expedited consultation process set out in rule A1.3. At the conclusion of the review, the ISO must publish a report containing any recommended changes to Subchapters 7.3 or 7.4 or the associated procedures.
- 2.1.2 Public consultation is an important part of the ISO’s transparent decision-making process, and the ISO welcomes stakeholder feedback on this draft decision or otherwise in relation to the processes set out in Subchapters 7.3 and 7.4 and the associated Procedures. All consultation will be undertaken in accordance with the ISO’s *Consultation Policy*.⁸
- 2.1.3 The ISO will take into account all in-time submissions and other comments. It will endeavour where practicable to consider late submissions.⁹ If you have missed a submission deadline but feel you have an important contribution to make, please contact the ISO promptly at info@pilbaraisoco.com.au.
- 2.1.4 The ISO is working to the following timetable:

Event	Date	Comments
Issues Paper	19 July 2024	Complete
Informal consultation	22 July 2024 – 9 August 2024	The ISO conducted a first informal round of stakeholder feedback.
Draft decision	4 October 2024	This document.
Formal written consultation	4 October 2024 – 1 November 2024	The ISO will allow a period of at least 15 Business Days for written submissions and comments on the draft decision (rule A1.3(b)).
Final decision and publication of report (rule 178(3))	Target November 2024	Final decision is to be within 20 Business Days after the end of the period allowed for making submissions and comments on the draft decision (rule A1.3(c)).

2.2 First round of consultation (completed) – informal feedback

- 2.2.1 In response to the Issues Paper, several stakeholders requested and were granted face-to-face meetings, and the ISO received three confidential informal submissions.
- 2.2.2 Appendix 1 summarises the key points from these meetings and submissions, and the ISO’s responses.
- 2.2.3 The ISO is grateful to those stakeholders for their input.

⁸ Available [here](#).

⁹ Under rule A1.6, the ISO may, but does not have to, take into account out-of-time submissions.

2.3 Second round of consultation (now) – Written submissions and comments

2.3.1 In accordance with the expedited consultation process required by rule 178(2), the ISO now seeks written submissions on this draft decision.¹⁰

2.4 Confidentiality and transparency

2.4.1 This draft decision proposes that the rules' confidentiality and transparency regime be rebalanced in favour of greater transparency (see section 4.3 below), but for the time being, stakeholders are reminded of the regime's existing rules regarding confidentiality.¹¹

2.4.2 The ISO's preference is for this review and associated stakeholder feedback to be as transparent as possible. Generally, written submissions received will be published on the ISO's website,¹² and the ISO has endeavoured to reflect all relevant informal feedback in this draft decision.

2.4.3 However, the ISO recognises that a stakeholder may wish to provide confidential information or make a confidential submission, in which case:

- (a) please clearly identify to the ISO which parts of any submission or feedback are confidential;
- (b) wherever possible please refrain from making blanket claims of confidentiality over an entire submission;
- (c) for any written submission, please also provide a redacted version for publication; and
- (d) the ISO will deal with any claims of confidentiality in accordance with rules A1.8 and A1.9.

2.5 Further Information

2.5.1 If you require any further information, please contact us at info@pilbaraisoco.com.au.

¹⁰ Rule A1.3(b)(ii)

¹¹ Subchapter 11.2, also rule 176 and rules A1.8 and A1.9.

¹² Rule A1.5

3. Case studies

3.1 About these case studies

- 3.1.1 This review is prospective. It is not the function of this review to report on or analyse specific past instances or outcomes, although of course experience from those past instances has informed some of the issues identified in the Issues Paper and discussed in this draft decision.
- 3.1.2 This section 3 sets out four hypothetical case studies to illustrate the issues discussed in this draft decision.
- 3.1.3 Although simplified and anonymized, these case studies are inspired by real-world NWIS incidents in the last 12 months.

3.2 Case study 1: Extended interconnector outage exposes region to contingent islanding risk

- 3.2.1 The NSP for a network (**network A**) needs to remove a network element from service for an extended period of over 6 months. The network element forms part of the interconnection between network A and another network (**network B**).
- 3.2.2 This changes the risk profile for a part of network B (the **relevant zone**), as follows:
 - (a) During the outage, the relevant zone will be serviced by two lines (**line B1** and **line B2**). Line B2 has a thermal capacity of only 25 MW.
 - (b) If line B1 were to trip, the relevant zone will be served by line B2 only. The zone's fate will thus depend on the load in the zone at the time. If the load is >25 MW, then line B2 will overload and trip, blacking out the zone.
- 3.2.3 NSP B judges that line B1 tripping is a credible risk, and so wishes to start a machine within the relevant zone whenever load in the zone is likely to exceed 25 MW. It regards the need to start this machine as having been caused by the network A outage, and so believes that the cost should be borne by NSP A or its network users. Because the outage in question lasts for many months, the cost involved is substantial.
- 3.2.4 In contrast, NSP A does not consider a loss of line B1 to be a credible risk, and so does not consider NSP B's machine start to be necessary. As a result, it does not wish to pay for it.
- 3.2.5 Discussions between the two NSPs and ISO do not resolve this impasse.
- 3.2.6 As an alternative solution, NSP B argues that the ISO can and should use its ESS procurement powers under Chapter 8 of the PNR, to contract for a suitable SRESS service under which the ISO control desk could direct machine starts as necessary to keep imports to the zone below 25 MW, thus mitigating the outage risk. It proposes that the cost of this ESS be distributed as usual, through the runway model in PNR rule 229. This alternative approach is discussed in section 8.5 below.

3.2.7 As identified in the Issues Paper, at present:

- (a) The PNR do not require the parties to use a common risk assessment methodology.¹³
- (b) Although the PNR require NSPs to seek to achieve consensus on system coordination matters,¹⁴ the PNR have no mechanism to resolve disagreements on risk assessment such as this.¹⁵
- (c) The PNR's definition of, and processes for, "pre-contingent threats" do not deal well with this form of proactive intervention.¹⁶
- (d) The PNR do not empower the ISO to determine what mitigations are (or are not) necessary to manage the risk associated with a planned outage.¹⁷
- (e) The PNR do not include a cost-recovery mechanism for any mitigation measures.¹⁸
- (f) It's unclear whether ESS can or should be used to mitigate outages (section 8.5 below). If they are, it's unclear whether the existing ESS cost allocation methods in PNR Subchapter 8.3 are appropriate.¹⁹

3.3 Case study 2: Transmission outage creating risk for another retailer's customers

3.3.1 The NSP for a network (**network X**) wishes to remove a network element from service.

3.3.2 This changes the risk profile for parts of network X and also parts of an interconnected network (**network Y**) (the **relevant zone**), because during the planned outage the relevant zone will be served by a single line (**line X1**).

3.3.3 NSP X and NSP Y both undertake a risk assessment in respect of the outage. Both agree that an outage on line X1 is low probability, but they differ in their assessment of its consequence. NSP X judges that an outage on line X1 would be of low consequence. In contrast, NSP Y judges that an outage on line X1 would be of extreme consequence, because its related gentailer business's customers in the relevant zone include the port operations of a major ore exporter.

3.3.4 Because of this disagreement over the risk assessment, NSP X and NSP Y are not able to agree on whether mitigation measures are required in respect of the planned outage, or who should pay for them.

¹³ Issues Paper, Issue 14.

¹⁴ PNR rule 170(d)

¹⁵ Issues Paper, Issues 9 & 12.

¹⁶ Issues Paper, Issue 17.

¹⁷ Issues Paper, Issues 18 & 22. At present the ISO must rely on the ISO control desk's ability to start a machine to provide SRESS under rule 214(2)(b).

¹⁸ Issues Paper, Issues 21 & 24. At present clause 3.14.7 of the EBAS Procedure fills this gap.

¹⁹ See discussion in section 8.5 of this draft decision.

3.3.5 As identified in the Issues Paper, at present:

- (a) The PNR have no mechanism to resolve this disagreement on the seriousness of risk consequences.²⁰
- (b) Due to limits on the scope of each NSP's network model, an NSP undertaking its own risk assessment may not be able to adequately identify or quantify an outage's impact in other networks.²¹
- (c) The PNR do not empower the ISO to determine what mitigations are or are not necessary to manage the risk associated with the planned outage.²²
- (d) The PNR do not empower the ISO to stop the outage until the matter is resolved or mitigations are in place.²³
- (e) NSP Y has no practicable path to intervene to prevent (what it judges to be) a serious risk to its network users' customers.²⁴

3.4 Case study 3: Unscheduled generator unavailability

3.4.1 An NSP (**NSP D**) has scheduled a planned outage in its network for a particular day.

3.4.2 Part of the risk mitigation plan for this outage includes the ability to call, if necessary, on the black start capabilities of a machine located in another network (**network E**). That machine is operated by the related gentailer business of network E's NSP (**NSP E**).

3.4.3 On the evening before the planned outage is scheduled to commence, NSP E notifies the ISO that its black-start capable machine is unavailable and will not be in service when NSP D's planned outage commences. The lack of a black-start capable machine could materially alter the planned outage's risk profile.

3.4.4 The ISO contacts NSP D and asks it to cancel the planned outage. NSP D refuses, and proceeds with the outage.

3.4.5 As identified in the Issues Paper, at present:

- (a) The PNR do not give the ISO a clear function of managing outages to preserve system security.²⁵

²⁰ Issues Paper, Issues 9 & 12.

²¹ Issues Paper, Issues 2, 6, 7 & 9.

²² See footnote 17

²³ Issues Paper, Issue 22.

²⁴ In theory NSP Y could perhaps commence an urgent rules dispute, seeking an urgent injunction to block the outage until the position was resolved, but this is obviously an unsatisfactory solution, and may well not be practicable.

²⁵ Issues Paper, Issues 1 & 22.

- (b) The PNR have no mechanism or Procedure for cancelling or recalling an outage, and the incident described does not fit comfortably into the definition of pre-contingent threat.²⁶
- (c) The PNR do not provide for the ISO's risk assessments to prevail.²⁷
- (d) The PNR do not require NSPs to comply with ISO directions regarding outages which may impact system security.²⁸

3.5 Case Study 4: Outage of a power station's ancillary equipment

- 3.5.1 The action in this case study takes place over a single weekend, starting on a Thursday and ending on the following Tuesday.
- 3.5.2 On the **Thursday**, in papers for the next day's system coordination meeting, an NSP advises the ISO of a planned outage in a piece of auxiliary equipment (the "**device**") in a power station on its network, scheduled to commence on the following Monday (i.e. in 4 days) and continue for roughly a week.
- 3.5.3 The power station has two of these devices and could operate at full power on either of them alone. Hence, the power station normally has N-1 redundancy on these devices. With one of them offline, the power station can still operate at full output, but will be at N-0 on the remaining device.
- 3.5.4 On the **Friday**, the system coordination meeting discusses the planned outage and the risk of UFLS events if the remaining device fails. The NSP undertakes to obtain information from the power station operator.
- 3.5.5 Early that Friday afternoon, the NSP advises the ISO that loss of the remaining device would cause complete loss of the power station.
- 3.5.6 Mid afternoon, the ISO informs the NSP that loss of the power station would likely involve a loss of generation greater than the 62 MW of SRESS currently contracted, leading to UFLS. Accordingly, the ISO asks the NSP to undertake a risk assessment and, if necessary, implement mitigation measures. The ISO suggests two possible mitigation measures the NSP could implement, including the NSP directing the relevant gentailer under rule 188(1) to rebalance its portfolio so that the power station in question remains below the 62 MW threshold. The ISO asks the NSP to share its risk assessment and proposed mitigations before the outage commences.
- 3.5.7 The issue remained unresolved early on **Monday** morning when the work was scheduled to commence. (In fact, unknown to the ISO, the work did not start until the Tuesday. The ISO only learned of this after it queried the NSP later that week.)

²⁶ Issues Paper, Issues 4, 7, 13, 14 & 22.

²⁷ Issues Paper, Issues 9, 18 and 19

²⁸ Issues Paper, Issues 22

- 3.5.8 On Monday morning, the NSP provides a risk assessment and informs the ISO that both the NSP and the power station operator consider the risk to be low, and hence that in its view no mitigations were required.
- 3.5.9 Around midday, the ISO writes to the NSP restating its view that the device's outage represents an unacceptable risk of UFLS, and expressing the view that the NSP should put mitigations in place. The ISO again suggests two possible mitigations.
- 3.5.10 Around 5pm, the NSP responds, stating that its advice on Friday that loss of the remaining device would cause loss of the whole power station was incorrect, and that in fact the power station could operate indefinitely (if sub-optimally) even with both devices offline.
- 3.5.11 Around 9am on **Tuesday**, the outage commences, despite the ISO's objections, without notice to the ISO and without the NSP having implemented the recommended mitigations.
- 3.5.12 Shortly after this, having re-assessed the risk based on the NSP's correction the previous evening (para 3.5.10), the ISO withdraws its request for the NSP to issue mitigating directions.
- 3.5.13 Although the matter was rendered moot by the NSP's Monday evening correction, it is worth noting that in that Monday response the NSP contends that:
- (a) It has not done a single point of failure assessment for auxiliary systems in the power station and so will not comment on whether the device was or was not normally designed to operate at N-1. It also observes that any power station likely had numerous single points of failure within its auxiliary systems, e.g. the main gas train.
 - (b) Because neither the PNR nor the HTR recognise an outage of power station auxiliary equipment as a "contingency", it has no power to issue directions under rule 188. (This is incorrect. The NSP's power to issue directions under rule 188(1) is not conditional on a "contingency" having occurred.)
 - (c) If the ISO wished it could establish a constraint rule to deal with the activity in question, under which the ISO control desk could then issue a constraint direction. (At the time, no constraint rule existed on which such a direction could be based and there was no way one could be put in place in time, under the processes in Subchapter 9.1.)
- 3.5.14 As noted, this paper does not propose to review rules participants' behaviour or assertions in respect of actual past events. This case study has been included because it shows that:
- (a) Outages are not being notified sufficiently in advance to enable orderly and prudent risk assessment and discussion. This increases the risk of error, as happened here.
 - (b) In circumstances where an NSP had notified the ISO of a potential risk of power station failure if it lost a device which would be operating at N-0 during planned works, and the ISO had notified the NSP that this represented an unacceptable risk of UFLS and advised the NSP not to proceed without adequate mitigations in place, the NSP nonetheless preferred its own risk assessment over the ISO's and proceeded with the outage without the mitigations.
 - (c) Outage of auxiliary equipment within a power station is not a "contingency" under the PNR.

- (d) The ISO had roughly half a working day, after being notified of an N-0 equipment status in which a failure could cause the power system to lose a block of generation greater than the available contracted SRESS, to undertake its own risk assessment (if this had been an ISO function under the rules and), liaise with affected parties, design mitigations, and arrange to have the mitigations put in place.

4. Structural matters

4.1 Introduction

- 4.1.1 During the informal consultation preceding this draft decision, and despite the difficulties experienced in the last 12 months as illustrated by the case studies in section 3, several stakeholders indicated that they felt the current processes and powers in Subchapters 7.3 and 7.4 were adequate, and that no rule changes (and in some cases no procedure changes) were necessary. As will be made clear in the following sections of this draft decision, the ISO does not agree.
- 4.1.2 But before turning to the detail of the rules, it's important to highlight two structural issues which exacerbate the weaknesses of the current regime.

4.2 Vertical integration

- 4.2.1 The first of these structural issues lies in the fact that all three of the registered NSPs are vertically integrated. Upstream of the networks, all three are generators. Downstream, APA and Horizon Power are retailers and Rio Tinto is a major consumer. Various parts of these businesses compete with each other.²⁹
- 4.2.2 Because of this vertical integration, there is a risk or perception that an NSP's operational decisions and risk assessments may be framed to favour its own upstream and downstream business and customers or disadvantage a competitor's. (There is also a concern that confidential information exchanged for outage* planning purposes might be exploited to gain an advantage in upstream or downstream markets—this is discussed in section 4.3 below.)
- 4.2.3 The PNR contain measures designed to mitigate these risks, including specifically in connection with Subchapters 7.3 and 7.4,³⁰ but some stakeholders have observed that these rules have limits.³¹
- 4.2.4 Whether and how the PNR and Pilbara ISOCO generally should be reformed to manage vertical integration and conflicts of interest is a matter for a broader review, but when it comes to outage coordination and management it's a subject this review can properly address, and the ISO agrees that the current mechanisms need reform in this regard. Specifically, recommendations in the following chapters propose that decisions which are currently made by the three vertically integrated NSPs either individually or collectively, should instead be made by the independent ISO.³²

²⁹ ACCC, *Draft Determination: Application for authorisation lodged by Pilbara ISOCO Ltd in respect of performing a function under the Pilbara Regime with the purpose of maintaining or improving power system safety, security or reliability - Authorisation number AA1000666*, 3 September 2024 (available [here](#)) (**ACCC Draft Determination**), paragraphs 4.2 to 4.6.

* *Reminder: References to outages in this draft decision generally include all notifiable events. See section 1.4.*

³⁰ PNR rule 176

³¹ See for example BHP's submission (available [here](#)) in connection with Pilbara ISOCO's 28 March 2024 application to the ACCC for authorisation.

³² EPWA's PNR Evolution review is considering whether the ISO's internal and external governance should be reformed to increase its perceived and actual independence: Pilbara Advisory Committee meeting papers for 29 August 2024 (available [here](#)), pdf pages 37-39.

- 4.2.5 But there is another aspect to vertical integration in an outage coordination context, namely its intersection with competition law.
- 4.2.6 Operating an interconnected system of multiple networks necessarily involves a degree of cooperation between the NSPs. But when those NSPs are vertically integrated, this need for cooperation creates a complication—some of the conduct involved in outage coordination could, in the absence of an exemption or authorisation, amount to illegal cartel conduct.³³
- 4.2.7 The Pilbara regime presently enjoys a statutory exemption from Part IV of the *Competition and Consumer Act 2010*.³⁴ That expires in November this year. The ISO is presently seeking an authorisation from the ACCC, and on 3 September 2024 the ACCC published a draft decision indicating that an authorisation may be granted. However, it remains to be seen whether this is reflected in a final decision, and even if an authorisation is granted it will be for a limited period and will be subject to various conditions with which stakeholders may or may not find compliance easy.³⁵
- 4.2.8 Whatever the ACCC outcome, it is up to each vertically integrated NSP (and each other rules participant) to determine how to fulfil its regulatory and operational obligations under the PNR without breaching the *Competition and Consumer Act 2010*. But the PNR should not make this task more difficult than it needs to be.
- 4.2.9 The crux of the competition risk lies in the PNR’s heavy emphasis on collaboration and cooperation, with the concomitant risk that the NSPs may reach agreement on a subject which amounts to an illegal “contract, arrangement or understanding” between competitors. This risk will be greatest when the PNR do not just *permit*, but actively *require*, the parties to try to reach agreement, as is the case with the present Subchapter 7.3 and 7.4 process.
- 4.2.10 A broader review may wish to address this problem more generally, but for the purposes of the present review, the ISO considers that it would be helpful for all concerned if NSPs were left with a *discretion* as to whether, how much and on what subjects they choose to discuss or seek agreement with their NSP colleagues. The PNR should not *compel* them to do so.
- 4.2.11 The ISO proposes to achieve this by moving the central decision-making responsibility under Subchapters 7.3 and 7.4 from the NSPs collectively, to the ISO. The ISO can still be informed by NSP consultation and even discussion, but if the decision is ultimately the ISO’s, there should be materially less risk of the NSPs reaching an illegal contract, arrangement or understanding. And if NSPs or others wish to abstain from discussions for competition risk or other reasons, the PNR should accommodate that wish without thereby compromising system security.

Draft Recommendation 1: That although Subchapters 7.3 and 7.4 should leave room for informal cooperation and collaboration between market participants, they should not require it.

³³ See discussion in Pilbara ISOCO’s 28 March 2024 application to the ACCC for authorisation (available [here](#)), paragraphs 127 – 153.

³⁴ *Electricity Industry (Pilbara Networks) Regulations 2021*, regulation 16A

³⁵ See ACCC Draft Determination, footnote 29 above.

4.3 Transparency

- 4.3.1 It's trite to observe that outage planning and management can have important consequences:
- (a) outages in one network can create risks for security and reliability for users of other networks, some of whom may be competitors of a vertically integrated NSP's upstream or downstream businesses;
 - (b) outages and their management can increase the cost of ESS for other market participants;
 - (c) outages can affect the short-term price of energy (especially but not only in systems with a regulated wholesale market)³⁶, and in extreme circumstances can result in market manipulation; and
 - (d) not least, the outage itself can involve a substantial work program with mobilisation timetables, etc, such that a disruption to the outage can be expensive.
- 4.3.2 In the European Union, outage planning information is classified as market-sensitive information, and its disclosure is regulated under the EU market transparency regime.³⁷ Both the WEM Rules and the NER have detailed regimes for the publication of outage information.
- 4.3.3 In contrast, the PNR have only limited transparency measures, and such information as is made available is not required to be distributed to all potentially affected participants, or to the public. There is a reason for this—some market participants consider outage information to be commercially sensitive information,³⁸ and the current PNR regime was designed to keep the information closely held.
- 4.3.4 The ISO considers that contrary to the current approach, information about outage planning should be as widely and transparently available as possible, to enable all market participants to assess any risks to their own business, and to take whatever mitigation measures they deem necessary. However, it acknowledges stakeholder concerns about the possible adverse consequences of this information being published, and accepts that there may be some instances where some information should be kept secret. This will require a careful balance to be struck, but the ISO believes that wherever possible the regime should favour transparency.
- 4.3.5 One side effect of greater transparency will be that the concerns about information leakage within vertically integrated NSPs will be diminished. Under the present regime, there is a concern that an NSP might exploit confidential information exchanged for outage planning purposes to gain an unfair or anti-competitive advantage in upstream or downstream markets. But if the information is publicly available, there will be no incentive for the network business to leak the information, and no advantage to its upstream or downstream business if it does so.

³⁶ Even in systems such as the NWS with no regulated wholesale market, a user faced with an outage will need to make alternative arrangements for supply to cover the outage, sometimes at short notice. This energy is likely to be more expensive than its normal long-term supply arrangements.

³⁷ See discussion of the REMIT arrangements in section 7.2.

³⁸ See for example BHP's (available [here](#)) and Woodside's (available [here](#)) submissions in connection with Pilbara ISCo's 28 March 2024 application to the ACCC for authorisation.

Draft Recommendation 2: That wherever possible, information about notifiable events should be publicly available. That in designing the detail of these rules, consideration should be given to whether any of this information needs to be kept confidential, and if so how transparency is nonetheless to be maximised.

- 4.3.6 In developing a rule change proposal to implement Draft Recommendation 2, the ISO will consult carefully with stakeholders as to what protections any transparency regime should retain for commercially sensitive information.

5. Definitions

5.1 “Outage” and “notifiable event”

- 5.1.1 The PNR definition of “**outage**” is expressed to include (at least³⁹) partial or complete unavailability or de-rating of equipment or a facility, whether planned or unplanned.⁴⁰
- 5.1.2 The PNR definition of “**notifiable event**” is broader, and includes not only planned outages, but also any other planned or anticipated system event which might credibly affect system security or reliability, the provision of ESS, or the provision of contracted transmission access.⁴¹ It explicitly includes commissioning and testing.⁴²
- 5.1.3 The PNR’s definition of “outage” matches the NER’s, which is simply “any full or partial unavailability of equipment or facility”.⁴³
- 5.1.4 In contrast, the WEM Rules have a complex definition for “outage” which begins with a functional concept (in simple terms, inability to respond to dispatch instructions) but then applies several carveouts, e.g. for intermittent generators if their intermittent energy source is unavailable.⁴⁴ The ISO does not consider this complexity to be necessary in the Pilbara regime, because it is primarily related to the management of facilities’ obligations under the WEM’s reserve capacity market.
- 5.1.5 The ISO does not consider that either of the PNR’s definitions of “outage” or “notifiable event” needs changing.
- 5.1.6 However, as discussed in the Issues Paper,⁴⁵ the way these definitions are *used* does need to change, because:
- (a) the overlap between “notifiable event” and “contingency” needs to be resolved;⁴⁶
 - (b) the ambiguity as to whether there is or is not (or should be) overlap between “notifiable event” and “pre-contingent threat” needs to be resolved;⁴⁷

³⁹ Because the definition of “outage” is open-ended (i.e. it is only an “includes” definition), it leaves open the theoretical possibility that some other things might also be “outages”. But the words used in the definition are already so broad that this theoretical possibility may have little practical effect.

⁴⁰ PNR rule 8

⁴¹ PNR rule 166

⁴² Unlike the definition of “outage”, the definition of “notifiable event” is closed, so there is no scope for the theoretical expansion as discussed in footnote 39. However, the words of rule 166 are already so broad, that this theoretical limitation may also have little practical effect.

⁴³ NER Chapter 10 Glossary

⁴⁴ WEM Rules rule 3.18.3

⁴⁵ Issues Paper section 5.1

⁴⁶ Issues Paper paragraphs 5.3.3 to 5.3.6

⁴⁷ Issues Paper paragraphs 5.3.7 to 5.3.8. The definition of “pre-contingent threat” in rule 8 is closed, being “an approaching external threat ... [an] impending material equipment failure, or ... an imminent risk of physical injury ... or ... damage”. It’s not easy to fit most planned outages into any of these categories. On the other hand, rule 186(1), which deals with the ISO’s pre-contingent functions, appears to regard planned outages as a species of pre-contingent threat.

- (c) there is overlap between “notifiable event” and the circumstances established under Chapter 8 in which ESS may be activated or machines enabled (see also section 8.5 below);
- (d) the Subchapter 7.3 and 7.4 processes may need to deal differently with different types of notifiable event, e.g. planned outages are in some ways different from commissioning and testing—when compared with other types of planned outage, commissioning and testing may require different cost allocation, timing of energisation, degree of advance notification, ranking in scheduling conflicts, etc;
- (e) the rules are not wholly consistent in how they refer to “planned outages” rather than “notifiable events”, which should be tidied up in any rule changes which arise from this review.

Draft Recommendation 3: That Subchapters 7.3 and 7.4 should enable the processes for notification, assessment, approval, scheduling and management of notifiable events to differentiate between and integrate across the various types of such events as appropriate, including:

- planned maintenance and routine upgrades;
- major or extended outages;
- commissioning and testing;
- events in integrated mining networks;
- events in the Pluto facility; and
- events in any other connection point compliance facility.

Draft Recommendation 4: That the PNR and Procedures should seek to minimise any risk of ambiguity, inconsistency or gaps arising from the potential overlap between:

- notifiable events being managed under Subchapters 7.3 and 7.4;
- contingencies and pre-contingent threats being managed under Subchapter 7.5 and the Protocol Framework; and
- the procurement and activation of ESS under Chapter 8.

Draft Recommendation 5: That the PNR’s and Procedures’ references to “outage” and “notifiable event” be made consistent.

- 5.1.7 Some of these matters should also be considered in a broader review. The ISO’s rule and procedure change proposals following this review will focus on Subchapters 7.3 and 7.4.

5.2 “System coordination matters”

- 5.2.1 **“System coordination matter”** is also defined very broadly, to include the scheduling and coordination of, and updates regarding, notifiable events, their likely impact on security, reliability and related matters, and their mitigation and management.⁴⁸

- 5.2.2 The ISO does not propose any change to this definition.

⁴⁸ PNR rule 167. As with the definition of “notifiable event”, this definition of “system coordination matter” is closed but is already so broad that the closure may have little practical effect.

- 5.2.3 The definition already encompasses the management and mitigation of events. As such, when Subchapters 7.3 and 7.4’s deficiencies in this respect are remedied (see section 8), the definition of “system coordination matters” will likely still be adequate as-is.

5.3 System states

- 5.3.1 Section 5.3 of the Issues Paper discussed some of the inconsistencies and illogic in the present rules’ treatment of this subject.
- 5.3.2 There is substantial overlap here with EPWA’s PNR Evolution review. The ISO does not propose any specific reforms at this point. It will consult further with EPWA and other stakeholders when it comes to drafting rule and procedure change proposals arising out of this review, to see whether improvements might be made in passing.

5.4 “Island”

- 5.4.1 The Issues Paper observed⁴⁹ that the rules currently treat islanding as a binary issue—either a portion of the network is in synchronous connection with the rest of the network, or it is not. In fact, recent experience in connection with a long duration planned outage (see Case Study 1, section 3.2) has demonstrated that management of notifiable events also needs to deal with situations in which synchronous connection remains in place, but the remaining interconnections are weak. In these circumstances interventions may be necessary, e.g. to prevent islanding or to ensure that if islanding does occur the island will remain secure.

Draft Recommendation 6: That the changes implemented under Draft Recommendations 3, 4 and 5 ensure that the limitations of the definition of “island” do not constrain the circumstances in which mitigation measures for notifiable events are considered or implemented.

- 5.4.2 This issue affects more than just outage management. For example it is also relevant to ESS procurement and activation. These aspects could be considered by a broader review.

⁴⁹ Issues Paper para 6.1.5

6. Objectives, functions and powers

6.1 Prioritising system security

- 6.1.1 Chapter 7 of the PNR deals with system operations. It commences with the “**system security objective**” which focusses on keeping the power system in, or returning it to, a secure state and inside the technical envelope. The ISO does not propose any change to this definition.⁵⁰
- 6.1.2 The problem is that this objective is not applied fully to Subchapters 7.3 and 7.4. As noted in the Issues Paper, the primary objective for Subchapters 7.3 and 7.4 in rule 173(1) contains three limbs being:
- (a) promoting communication and collaboration;
 - (b) provision of sufficient information to enable rules participants to perform their functions; and
 - (c) promoting collaborative resolution of scheduling conflicts and other matters.
- 6.1.3 The secondary objective in rule 173(2) focusses on efficiency and informality.
- 6.1.4 The system security objective is mentioned only indirectly and in a limited fashion, as the yardstick for assessing the provision of information in the second limb of the primary objective.
- 6.1.5 This is inadequate. The primary objective for all parties engaged in outage* planning, notification, assessment and management should be to preserve security and reliability. To illustrate: In Draft Recommendations 12, 15 and 16 below, the ISO proposes that it be given suitable powers to issue directions. Under rule 173(1) as currently drafted, these powers arguably could only be used to promote communication, collaboration and information provision—they arguably could not be used for other interventions such as making decisions when collaboration fails, or directing active operational steps such as starting a machine.
- 6.1.6 Accordingly, rule 173(1) should be reframed. A useful precedent is rule 184(1), which sets the objective for Subchapter 7.5 as being simply “to achieve the system security objective”.
- 6.1.7 Recasting the primary objective for Subchapters 7.3 and 7.4 in this fashion poses the question of whether the current emphasis on collaboration and communication should be retained, for example by being merged into the secondary objective in rule 173(2). This is a matter of detail which can be considered during detailed rule drafting, and it will also no doubt form part of a broader review. But as the other recommendations in this draft decision make clear, the ISO considers that the present

⁵⁰ A stakeholder did suggest that the third limb of this objective (to otherwise maintain and seek to improve security and reliability) could be read independently from the first two limbs, and that its reference to “improve” was sufficient to give the ISO the power it needs to manage outages. For the reasons set out in the introduction to rows 48 to 56 in Appendix 1, the ISO will not be relying on this interpretation, and so does not need to express a concluded view on its merits. That said, the ISO is inclined to the view that the word “otherwise” at the beginning of paragraph (c) makes it reasonably clear that the primary focus of the system security objective is found in paragraphs (a) and (b), and that that word’s presence would make it difficult to give paragraph (c)’s reference to “improve” some higher or broader status. A subsequent rule change process might wish to consider whether rule 162(c) should include the word “improve”, but for the time being the ISO regards the language of the system security objective as an out-of-scope side issue for this review.

* *Reminder: References to outages in this draft decision generally include all notifiable events. See section 1.4.*

regime places too much emphasis on collaboration, at the expense of there being no clear decision-maker on critical matters, and at the expense also of exacerbating the competition risk associated with NSPs' vertical integration. For these reasons, the ISO is inclined to the view that the secondary objective in rule 173(2) is adequate as is. Its goal of informality and efficiency, and maximising communication while minimising the compliance burden, seems sufficient to allow the outage regime to use collaboration where appropriate, without compelling it where it's inappropriate.

Draft Recommendation 7: That the primary objective for Subchapters 7.3 and 7.4 be revised, to focus solely on achieving the system security objective.

- 6.1.8 On this subject, the Issues Paper noted that one stakeholder had suggested to it that rules participants' system security obligations should be suspended during a notifiable event.⁵¹ The ISO does not consider this appropriate. Rule 172 sets out the circumstances in which a participant may be relieved from its system security obligations, and the ISO proposes no change to that rule.

6.2 Clear role for the ISO to assess, coordinate and oversee management of notifiable events

- 6.2.1 By design, the present rules do not clearly specify any one person as being responsible for, or having clear powers in respect of, outage coordination and planning. Rather, that task is left to the NSPs individually, overseen to some extent by collective discussion at the system coordination meeting.
- 6.2.2 In contrast, the ISO's role regarding outages appears deliberately constrained:
- (a) At the highest level, it is true, rule 32(1) restates the ISO's general system security function under the Act—to maintain and improve system security in the NWIS and any other interconnected Pilbara network.
 - (b) But when it comes to notifiable events, although rule 33(1)(j) does give the ISO a general function of undertaking system coordination and outage scheduling, this is not as broad as may at first appear because:
 - (i) it is limited by the qualification that this be done "under" (i.e. in accordance with)⁵² Subchapters 7.3 and 7.4, so that it would be difficult to use this provision to expand on those Subchapters if they omit a function;
 - (ii) it refers only to "system coordination" and "outage *scheduling*"—it notably does not refer to outage (or notifiable event) approval, assessment or management;
 - (c) Subchapters 7.3 and 7.4 themselves set out a deliberately narrow role for the ISO, limited to:
 - (i) convening and chairing system coordination meetings;⁵³

⁵¹ Issues Paper paragraphs 6.2.8 to 6.2.10

⁵² rule 9(1)(o)

⁵³ rule 174

- (ii) between meetings, liaising on system coordination matters;⁵⁴
- (iii) producing system coordination reports, in which the ISO's role is limited to expressing opinions⁵⁵ and making "recommendations"⁵⁶;
- (iv) resolving scheduling conflicts between an outage and any other notifiable events, ideally by consensus but as a last resort by direction.⁵⁷

6.2.3 To emphasise the ISO's limited role, the rules explicitly state that the ISO does *not* have a general obligation to "investigate" (which likely includes assess) notifiable events beyond information provided to it by NSPs.⁵⁸ Further, the explicit granting of a power to issue directions in connection with scheduling conflicts, raises an inference that the ISO does not otherwise have a power to issue directions under Subchapters 7.3 and 7.4 where no scheduling conflict arises.⁵⁹

6.2.4 Similarly, except for unplanned outages, the rules provide no regular⁶⁰ mechanism for the ISO to interact directly with registered controllers of either generators or loads, even if they may be materially impacted by an outage (see Case Studies 2 and 4).

6.2.5 As the case studies in section 3 show, this very narrow role for the ISO has created circumstances where there is no-one to resolve disagreements between NSPs over risk or mitigation, no-one to stop an NSP from proceeding with an outage which the ISO has determined poses an unacceptable risk, and no-one to make a final determination that mitigation measures are necessary, or, having made that determination, to direct that they be implemented.

6.2.6 This is unacceptable. There needs to be a clear single authority with the power to resolve these matters. The ISO is the logical choice for that role.

Draft Recommendation 8: That the ISO be given the overarching function of managing and approving notifiable events, including supervising their notification and scheduling, assessing their risks, and supervising, and as necessary directing, the management (including mitigation) of those risks.

6.2.7 The ISO is not currently resourced for this function. That should be addressed.

Draft Recommendation 9: That the ISO develop its own resources to deliver the function described in Draft Recommendation 8.

⁵⁴ rule 175

⁵⁵ rule 177(1)(b) ("any follow-up actions the ISO considers appropriate")

⁵⁶ rule 177(1)(c)

⁵⁷ rule 182

⁵⁸ Second limb of rule 177(4), which states that the ISO need not investigate beyond the sources of information listed in rule 177(3). Those sources are (a) system coordination meetings (generally attended only by the ISO and NSPs), (b) NSPs' internal outage planning reports; and (c) other information provided by NSPs.

⁵⁹ One submission to the ISO sought to interpret "scheduling conflict" very broadly, as encompassing any situation in which there was disagreement about the assessment or management of an outage. The ISO does not consider this interpretation to be available under the definition of that term in rule 182(1).

⁶⁰ They can be invited to attend system coordination meetings on an ad hoc basis: see {note} below rule 174(4)(d).

6.3 Re-focussed role for the ISO Control Desk

- 6.3.1 At present, by design, the ISO is a very small organisation with minimal staff.
- 6.3.2 Over the last few years, the ISO has found itself needing within short time frames to do its own technical risk assessment, so that it can try to referee disagreements over outage planning, risk assessment and mitigation.
- 6.3.3 The ISO has on occasion been forced to call on the technical expertise of the ISO control desk to help it in this regard.
- 6.3.4 This is undesirable because:
- (a) if Horizon Power is one of the parties to a disagreement about outages, then despite whatever internal ringfencing arrangements may be in place:
 - (i) the control desk staff are placed in the difficult position of helping the ISO resolve a disagreement between their employer and another NSP; and
 - (ii) doubts will arise as to the independence of the advice the ISO is receiving;
 - (b) although the current control desk staff are very experienced, they do not have access to the necessary whole of system models to undertake objective risk assessments; and
 - (c) it arguably falls outside the scope of the functions the rules envisaged would be delegated to ISO control desk, which were limited to "real time" functions.⁶¹
- 6.3.5 The ISO considers that the boundary lines should be redrawn, such that the ISO control desk's functions are limited to real-time and related matters, and the ISO in its own right takes on its responsibility for these planning and anticipatory activities.

Draft Recommendation 10: That the ISO control desk's functions be restricted to real-time operations, contingency response and managing near-term pre-contingent threats such as cyclones and bushfires.

6.4 Standardised risk assessment

- 6.4.1 The NWIS lacks a standardised risk assessment framework. This has given rise to difficulties on several occasions. There will always be scope for differences of opinion on risks and consequences, but it should not be possible for two NSPs, having agreed on the probability of a risk, to reach diametrically opposed assessments of its severity, as happened in Case Study 2 (section 3.3).
- 6.4.2 Several stakeholders have recommended that the ISO should develop a single, common risk-assessment framework as AEMO has done under the NER and WEM, and that all participants should be required to use this framework. The ISO agrees.

⁶¹ rule 45

Draft Recommendation 11: That the rules or a procedure require the ISO to develop a standardised risk assessment framework for assessment, approval, scheduling and management of notifiable events, and require all participants to use that framework.

6.5 Adequate powers to intervene

- 6.5.1 The case studies in section 3 illustrate that the current Subchapter 7.3 and 7.4 processes, which rely primarily upon collaboration between NSPs, cannot be relied upon to produce consensus outcomes in all circumstances.
- 6.5.2 It's clear that there must be one authoritative voice to resolve disagreements over risks and mitigation, to determine what mitigations are appropriate, to require the relevant participants to implement these mitigations, and to prevent outages from proceeding if the risks are excessive and there are not adequate mitigations in place. The ISO is the logical choice for that role.

Draft Recommendation 12: That the rules and procedures give the ISO the necessary powers to give directions in connection with the scheduling and management of notifiable events. That this include a power to approve or disapprove notifiable events with or without conditions, and a power to recall equipment where appropriate.

6.6 An outage* management procedure

- 6.6.1 The PNR, like the NER and the WEM Rules, adopt a model in which the rules set out core functions, obligations and requirements, but leave the finer operational details to a procedure.
- 6.6.2 However, the PNR lack a procedure to support Subchapters 7.3 and 7.4.
- 6.6.3 The ISO proposes that the process for notification, assessment, coordination, approval, and management (including mitigation) of outages be documented in considerably more detail than is presently the case. Participants' functions, responsibilities and powers should be more clearly articulated.
- 6.6.4 While the core aspects of this regime should be set out in rules, it would be sensible for the ISO to have a procedure-making power in this regard, to allow greater flexibility on some of the finer operational detail.
- 6.6.5 The question of which aspects should go in the rules, and which in the procedure, can be resolved during the detailed rule change and procedure development process. As a guide, the ISO expects that the NWIS regime may follow the broad delineation between rules content and procedure content found in the SWIS, although the NWIS outage regime need not be as complex.

Draft Recommendation 13: That the ISO develop a new Procedure to govern the notification, assessment, approval, scheduling and management of notifiable events.

* *Reminder: References to outages in this draft decision generally include all notifiable events. See section 1.4.*

6.6.6 At the same time the ISO will make consequential changes to its existing procedures, in particular the *Interim Access and Connection Procedure*, the *Interim Protocol Framework Procedure* and the *Interim Energy Balancing and Settlement Procedure*.

7. The outage* planning and assessment process

7.1 The current process

7.1.1 The current process under Subchapters 7.3 and 7.4 is minimal and relies heavily on registered NSP's autonomous conduct.

Notification of events

7.1.2 Each registered NSP must notify the ISO of each planned or anticipated notifiable event, and any changes in a previously notified event.⁶²

7.1.3 This notification may be given orally at the next system coordination meeting.⁶³ The note to this rule indicates an expectation that the notification would be given "as soon as the event appears on the NSP's planning horizon". In practice, system coordination meetings tend to focus mainly on the upcoming 14 days.

7.1.4 The NSP must also give the ISO a copy of its internal planning report for each notifiable event.⁶⁴ The ISO is to use this in preparing its fortnightly system coordination report.⁶⁵

7.1.5 In practice outages are now scheduled centrally in a database owned by one of the NSPs.

7.1.6 If a notifiable event arises and is likely to occur before the next system coordination meeting, the NSP must take reasonable steps to inform and coordinate with other registered NSPs, the ISO and the ISO control desk regarding the event.⁶⁶

7.1.7 Each registered NSP is responsible for keeping itself sufficiently informed of outages of facilities connected to its network, to enable it to comply with its obligations under Subchapters 7.3 and 7.4.⁶⁷ There is a complementary obligation on registered controllers (of generation and large loads) to keep their NSP informed.⁶⁸ There is no obligation on registered controllers to share this information with the ISO.

7.1.8 There is a separate notification obligation for unplanned outages—registered NSPs, generators and ESS providers must promptly on a 24/7 basis notify other registered NSPs and the ISO control desk of any contingency or unplanned outage⁶⁹ which may jeopardise system security, the provision of ESS or access services on a covered network.⁷⁰ This is the only part of Subchapters 7.3 and 7.4 for which a

* *Reminder: References to outages in this draft decision generally include all notifiable events. See section 1.4.*

⁶² rule 180(1)

⁶³ rule 180(2)(a)

⁶⁴ rule 180(2)(b)

⁶⁵ rule 177(3)(b).

⁶⁶ rule 179(1)

⁶⁷ rule 181(1)

⁶⁸ rule 181(2)

⁶⁹ As a minor drafting point, the definition of "**notifiable unplanned event**" in rule 183(5) is too broad. It encompasses "any ... event ... which might credibly be expected to adversely affect ... the System Security Objective", which on its face would also catch all planned events. Whether this overlap needs to be tidied up will depend on how other rule changes might be drafted.

⁷⁰ rule 183.

Procedure is available—the communication of unplanned outages may be regulated under the Protocol Framework.⁷¹

Process

- 7.1.9 The primary mechanism for outage planning is the fortnightly “**system coordination meeting**”. This meeting must discuss all “**system coordination matters**”, which includes the scheduling, coordination and management of all notifiable events, including any changed circumstances regarding a previously discussed notifiable event, and anything else relevant to security and reliability.⁷²
- 7.1.10 Generally, only NSPs and the ISO attend system coordination meetings. Meetings should last 30 minutes unless agreed otherwise.⁷³
- 7.1.11 Between meetings, the ISO is to liaise as necessary with NSPs and registered controllers.⁷⁴
- 7.1.12 After each meeting, the ISO is to produce a “**system coordination report**”, which is to report on all current or anticipated system coordination matters, any follow-up actions the ISO considers appropriate, and any recommendations the ISO has in respect of these matters.⁷⁵ The ISO’s recommendations in this report have no binding force.
- 7.1.13 The ISO’s system coordination report may rely entirely on information provided by NSPs. The rules state explicitly that the ISO does not have to undertake any investigations of its own.⁷⁶
- 7.1.14 The system coordination report is given to registered NSPs and to ESS providers.⁷⁷ It is not given to other rules participants and is not published.
- 7.1.15 There is a separate mechanism for “**scheduling conflicts**”. A scheduling conflict arises only when the ISO determines that an “outage” (not, in this case, a notifiable event), taken together with all other current or anticipated notifiable events may:
- (a) cause the system to be outside the technical envelope; or
 - (b) otherwise pose an unacceptable risk to security or reliability.
- 7.1.16 The rules do not specify any process for the ISO to make the determination of whether a scheduling conflict exists, but the ISO could use the power system model for this purpose,⁷⁸ if there was time to do so.

⁷¹ rule 183(4). The “**Protocol Framework**” is a Procedure developed under Subchapter 3.7 to deal with contingencies and pre-contingent threats. It is used in real-time operations under Subchapter 7.5.

⁷² rule 167

⁷³ rule 174

⁷⁴ rule 175

⁷⁵ rule 177

⁷⁶ rule 177(4)

⁷⁷ rule 177

⁷⁸ rule 109. Subchapters 7.3 and 7.4 are not explicitly listed in rule 108(2) as one of the things the power system model must be able to help the ISO with, except in the catch-all in rule 108(2)(k), but this does not limit the scope of rule 109. Rule 108 describes the requirements for the model’s capability. Rule 109 sets out the (broad) scope of the ISO’s power to use it.

- 7.1.17 Scheduling conflicts are to be resolved by consensus wherever possible.⁷⁹ The ISO’s power to give directions does not arise until the ISO has first determined that a consensus will not be reached in time for the relevant events to be managed appropriately.⁸⁰
- 7.1.18 Once this threshold is passed, the ISO may give a direction. The scope of the ISO’s power to give directions is unclear:
- (a) Directions may be given to “the affected parties”. This expression is unclear—does it mean only the entities planning the conflicting outages, or does it mean anyone who may be impacted by the resulting loss of security if the conflict were allowed to materialise? What does seem clear is that the ISO cannot issue a direction to any non-affected rules participant (i.e. someone not involved in the scheduling conflict or likely to be adversely affected), which seems to preclude the ISO from directing another generator to start a machine.
 - (b) The scope of directions is also ambiguous. A direction may “may specify which Notifiable Event is to have priority for scheduling purposes, and may contain such scheduling or other information or instructions as the ISO considers reasonably necessary to resolve the Scheduling Conflict and achieve the System Security Objective”.⁸¹ Most of this language is restricted to scheduling and the provision of information, which aligns with the narrow scope of the Subchapter 7.3 and 7.4 objective discussed above. On the other hand, it is possible to read these words as including a very broad scope: “may contain such ... instructions as the ISO considers reasonably necessary to ... achieve the System Security Objective”.⁸² This ambiguity should be resolved.

7.2 Outage management under other regimes

- 7.2.1 The ISO saw little benefit in undertaking a comprehensive review of the world’s outage management processes. The proposed outage process described in section 7.3 is a simplified version of the current WEM Rules process (described below), informed by a high-level review of the process in the *National Electricity Rules* and the European Union’s outage transparency mechanisms.

WEM Rules

- 7.2.2 The WEM Rules process is a logical starting point because:
- (a) it is created under the same Act as the PNR;
 - (b) it is administered by the same rule-making body (the Coordinator); and
 - (c) it has recently been modified after extensive review and stakeholder engagement.

⁷⁹ rule 182(2)

⁸⁰ rule 182(3)

⁸¹ rule 182(5)

⁸² The question confronting this broad interpretation is whether the word “instructions” should be read down by its context, appearing as it does after two references to only scheduling matters.

7.2.3 However, it was important to simplify and modify the WEM Rules process because:

- (a) the WEM Rules process contains more complexity than Pilbara needs—for example the WEM process has rules for self-scheduling facilities, mandatory routine maintenance, opportunistic maintenance, market impacts and compensation, which are necessary in the WEM to manage the outage process’s interactions with various other parts of the WEM (such as the reserve capacity mechanism, centralised dispatch and the wholesale market) which the Pilbara lacks;
- (b) the SWIS has only a single NSP, which is not vertically integrated;
- (c) the NWIS is presently a much smaller and simpler system;
- (d) the NWIS has special arrangements for integrated mining networks and the Pluto facility.

7.2.4 The WEM Rules process⁸³ is described in section 6.5 of AEMO’s Market Design Summary,⁸⁴ which is reproduced in **Appendix 3** to this draft decision.

7.2.5 In the WEM Rules, in addition to managing the outages themselves, outage scheduling is a key input to the Medium Term and Short Term PASAs (projected assessment of system adequacy). The Medium Term PASA gives a rolling weekly 36 month look-ahead, and the Short Term PASA gives a rolling daily 7-day look-ahead.

National Electricity Rules

7.2.6 AEMO describes the general principles governing its NEM transmission outage assessment as follows:

AEMO will only allow an outage to proceed on the basis that the outage will not result in a power system security or reliable operating state violation. Consideration must also be given to what actions would be required to return the power system to a secure operating state within thirty minutes following a credible contingency event or a significant change in power system conditions during the outage period. This principle applies to all outages including concurrent and/or high impact outages.⁸⁵

7.2.7 As in the WEM Rules, in addition to managing outages themselves, the NER outage process provides a key input to the Medium Term and Short Term PASAs.

7.2.8 The NER process for transmission outages commences with the NSP posting details of its proposed outage on AEMO’s public Outage Schedule.⁸⁶ This is done up to 2 years in advance.

⁸³ See *WEM Rules* clauses 3.18 to 3.20, and *AEMO WEM Procedure: Outages*, 1 October 2023 (available [here](#)).

⁸⁴ *AEMO Wholesale Electricity Market Design Summary*, September 2023 (available [here](#)), section 6.5.

⁸⁵ *AEMO Outage Assessment* (document reference SO_OP_3718), 3 June 2024, available [here](#) (***NEM Outage Assessment Procedure***), p. 5. Italicisation removed.

⁸⁶ Available [here](#).

- 7.2.9 In addition each NSP must provide information for AEMO to publish in its 13-month outage plan, as part of its *Congestion Information Resource*,⁸⁷ and any necessary limit advice⁸⁸ to enable AEMO (where possible⁸⁹) to determine the necessary constraint equations which will apply during the outage.⁹⁰
- 7.2.10 AEMO then assesses each outage, and determines what network constraints may need to be implemented while the outage is under way.⁹¹
- 7.2.11 Once AEMO has completed its assessment, the Outage Schedule will be updated, giving the proposed outage's status. Statuses include:⁹²
- (a) MTLTP - Medium Term Likely to Proceed. The outage has been assessed in the medium term by AEMO (24 months to 8 days ahead) and it is likely to proceed.
 - (b) STLTP - Short Term Likely to Proceed. The outage has been assessed in the short term by AEMO (7 to 1 days ahead) and is likely to proceed.
 - (c) PDLTP - Pre-Dispatch Likely to Proceed. The outage has been assessed in pre-dispatch by AEMO (40 to zero hours ahead) and is likely to proceed.
 - (d) PTP - Permission to Proceed. The outage has been given permission by AEMO to begin.
 - (e) PTR - Permission to Restore. The outage has been given permission by AEMO for restoration to begin.
 - (f) ISSUES - Assessment has taken place and an issue has been identified. The issue must be addressed before the outage can proceed.
 - (g) UTP - Unlikely to Proceed. The issue remains unresolved.
- 7.2.12 AEMO will continue to monitor the Outage Schedule and other factors. Permission to proceed (PTP) is not given until immediately before the scheduled start time, and remains valid for only 15 minutes because network conditions can change.⁹³ AEMO may reclassify an outage from LTP to UTP at any time.⁹⁴ ISO understands that an outage will usually only be classified as unlikely to proceed (UTP) if AEMO judges that there is likely to be a material lack of reserves (LOR2 or LOR3), or if some other precondition for the outage has not been satisfied, e.g. another piece of equipment needed to have returned from outage, but has not.
- 7.2.13 It is up to each NSP to make its own risk assessment of whether to mobilise crews etc for an LTP outage, i.e. whether the control desk is likely to grant permission to proceed. This assessment will be based on a range of factors including the Medium Term and Short Term PASAs, ongoing

⁸⁷ AEMO *Congestion Information Resource Guidelines*, 20 October 2021, available [here](#), section 3.2.2.

⁸⁸ AEMO *Limits Advice Guidelines*, 30 March 2012, available [here](#), section 4.

⁸⁹ AEMO *Constraint Formulation Guidelines*, 22 June 2023, available [here](#) (**NEM Constraint Formulation Guidelines**), section 8.3.

⁹⁰ *NEM Constraint Formulation Guidelines* (see footnote 89), section 3.2.

⁹¹ *NEM Outage Assessment Procedure* (see footnote 85), section 8.

⁹² This summary adapted from AEMO website, [here](#).

⁹³ *NEM Outage Assessment Procedure* (see footnote 85), section 9.15

⁹⁴ *NEM Outage Assessment Procedure* (see footnote 85), section 9.16

communication with AEMO, the constraints AEMO has identified as being associated with the outage, weather forecasts, and the like. The ISO understands that NSPs are generally able to make reasonably accurate predictions in this regard.

7.2.14 Like the NWIS, the NEM comprises multiple interconnected networks with separate operators. There are special rules for dealing with outages on interconnectors.⁹⁵

7.2.15 The NER outage management process and timeline are summarised in Figure 2 and Figure 3 respectively:

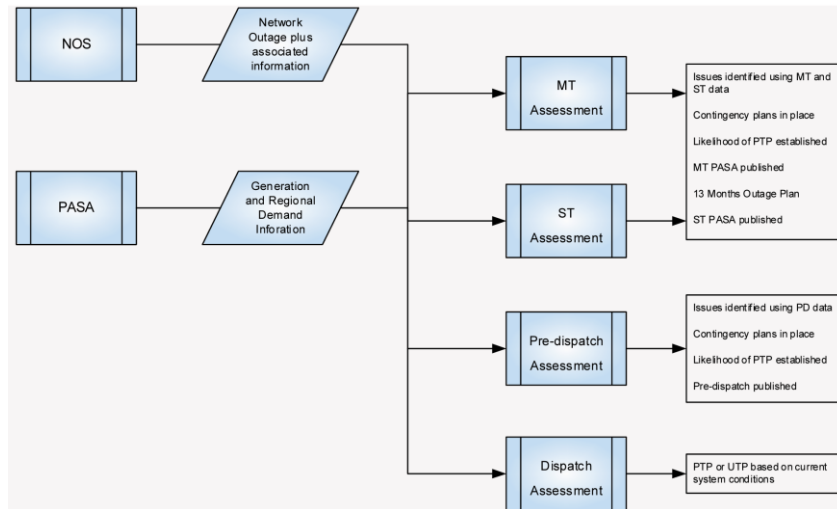


Figure 2 - NER outage process⁹⁶

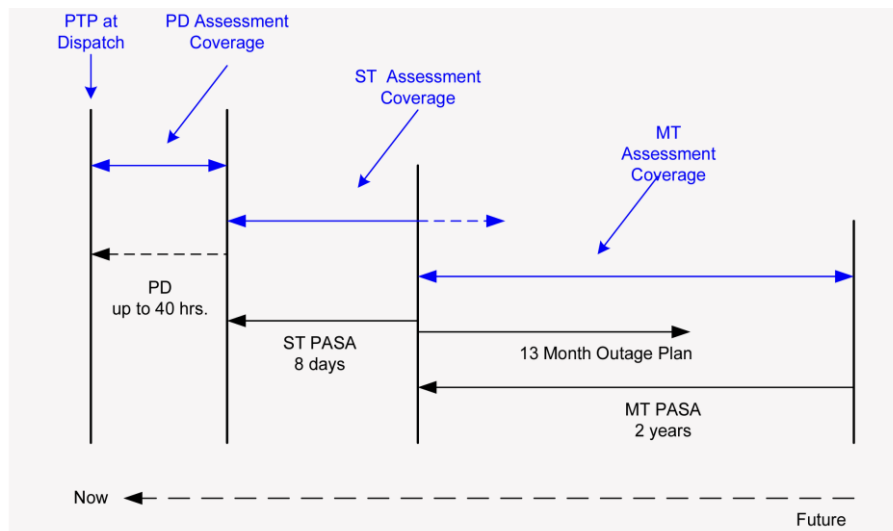


Figure 3 - NER outage timeline⁹⁷

⁹⁵ NEM Outage Assessment Procedure (see footnote 85), section 10

⁹⁶ AEMO Outage Assessment (document reference SO_OP_3718), 3 June 2024, available [here](#), Figure 1, p. 6.

⁹⁷ AEMO Outage Assessment (document reference SO_OP_3718), 3 June 2024, available [here](#), Figure 2, p. 8.

- 7.2.16 One important observation from the NER process is how closely outage management needs to be integrated with network constraint management. That subject is beyond the scope of this review. EPWA is considering network constraints as part of both its PNR Evolution review⁹⁸ and the grid transformation being discussed through its Pilbara Roundtable process.⁹⁹
- 7.2.17 Another observation is that, at least ostensibly, the NER outage process focusses on transmission outages and does not give AEMO a similar role regulating generator outages. The ISO understands this to be a design decision based on: first, the regime’s designers considering that the NEM’s wholesale spot price would send a price signal to generators to schedule outages at times of low system demand; and second, that the large number of generators installed across the NEM provided ample redundancy. Neither of these applies in the NWIS.
- 7.2.18 Further, the ISO understands that although there is no formal process for managing generator outages, in practice generation plant operators, especially for synchronous plants, do tend to discuss their planned outages with AEMO because even though AEMO lacks an explicit *approval* power in respect of such outages, it does have a *power to recall* a generator from outage including, if necessary, immediately after the outage commences.
- 7.2.19 Accordingly, the ISO considers that the NWIS outage management regime should extend to registered generators (see para 7.3.3 below).

European Union

- 7.2.20 The European regime offers another example of how to manage outages across multiple networks, although the regulatory environment is more complex than the NEM because each jurisdiction’s network is governed by that nation’s individual laws.
- 7.2.21 This review has not analysed the EU outage regime in detail, but aspects of it offer useful parallels and perspectives.
- 7.2.22 In the EU, outage management is seen as a vital component of market integrity and transparency, within the overarching “REMIT” (Regulation on Wholesale Energy Market Integrity and Transparency) scheme.^{100,101} Violation of REMIT rules can amount to insider trading or market manipulation, and can carry serious consequences for companies and jail time for individuals.
- 7.2.23 The ISO considers this a useful perspective. The fact that the EU regulates outages through the REMIT mechanism emphasises that outage management is not just a technical operational matter—it is a critical enabler of an effective and transparent market.

⁹⁸ Pilbara Advisory Committee meeting papers for 29 August 2024 (available [here](#)), pdf page 34.

⁹⁹ DEMIRS, *Pilbara Energy Transition - Request for Expressions of Interest for Priority Projects - Application Guidelines*, available [here](#), Appendix A.1.5(e).

¹⁰⁰ General information about REMIT can be found [here](#).

¹⁰¹ The overarching regulatory instrument for REMIT is *Commission Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency*, available [here](#).

7.2.24 The EU regime is housed in the *Guideline on electricity transmission system operation*,¹⁰² which gives useful guidance on how to regulate outages across multiple networks and NSPs:

- (a) The EU outage regime regulates “**TSOs**” which are equivalent to the Pilbara’s “NSPs” or the NEM’s “TNSPs”. Most nations have a single TSO, some have a small handful.¹⁰³
- (b) The EU grid is divided into “capacity calculation regions” for the purposes of capacity allocation and congestion management.¹⁰⁴ For example the “core” region comprises Ireland, France, Belgium, The Netherlands, Germany, Austria, the Czech Republic, Poland, Slovakia, Hungary and Romania. The NWIS can be considered a single such region.
- (c) All TSOs within a capacity calculation region (by analogy, all NSPs within the NWIS) must appoint a “**regional security coordinator**” (by analogy, the ISO) who will be delegated responsibility for, among other things:¹⁰⁵
 - (i) year-ahead, day-ahead and intraday operational security coordination including contingency response¹⁰⁶;
 - (ii) building a common grid model;¹⁰⁷
 - (iii) regional adequacy assessment;¹⁰⁸ and
 - (iv) relevantly, outage coordination.
- (d) To help with outage coordination, each TSO must provide information:
 - (i) it must give the regional security coordinator “the information necessary to detect and solve regional outage planning incompatibilities, including at least ... the availability plans of all its internal relevant assets”;¹⁰⁹ and
 - (ii) it must give all other TSOs in the outage coordination region “all relevant information at its disposal on the infrastructure projects related to the transmission system ... power generating modules, or demand facilities that may have an impact on the operation of the control area of another TSO within the outage coordination region”.¹¹⁰

¹⁰² *Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (EU Transmission Operation Guideline)*, available [here](#).

¹⁰³ <https://www.entsoe.eu/about/inside-entsoe/members/>

¹⁰⁴ See interactive map of the CCRs [here](#). They are created under *Commission Regulation (EU) 2015/1222 of 24 July 2015 establishing a guideline on capacity allocation and congestion management*, available [here](#).

¹⁰⁵ *EU Transmission Operation Guideline* (see footnote **Error! Bookmark not defined.** above), Article 77.

¹⁰⁶ *ibid*, Article 78.

¹⁰⁷ *ibid*, Article 79.

¹⁰⁸ *ibid*, Article 81.

¹⁰⁹ *ibid*, Article 80(3)

¹¹⁰ *ibid*, Article 83(4)

- (e) All TSOs, supported by the regional security coordinator, must perform outage coordination to ensure the operational security of the transmission system.¹¹¹
- (f) To facilitate this the TSOs must develop and comply with a joint outage coordination procedure which specifies the requirements for at least year-ahead and week-ahead coordination.¹¹² The EU regime provides detailed rules for the year-ahead process.¹¹³

7.2.25 The EU regime has a mechanism to deal with a situation in which TSOs cannot reach agreement on how to resolve an outage planning incompatibility—in this situation each TSO must force the relevant asset to be available, i.e. the outage cannot proceed.¹¹⁴ Although expressed differently (force the asset to be available), this is the same outcome as in the NEM and the WEM—an outage cannot proceed until the risks are adequately managed.

7.3 Recommended process for Pilbara

7.3.1 Taking account of the above, the ISO considers that a suitable outage management process for Pilbara in the near term is the following.

Draft Recommendation 14: That a notifiable event management process be established for the NWIS as described in this section 7.3.

Note: The following is a narrative description, not detailed rule drafting.

Overview

7.3.2 The proposed process can be shown schematically as shown in Figure 4:

¹¹¹ *ibid*, Article 82

¹¹² *ibid*, Article 83(1) (develop) and (2) (comply with)

¹¹³ *ibid*, Articles 91-100

¹¹⁴ *ibid*, Article 98(4)

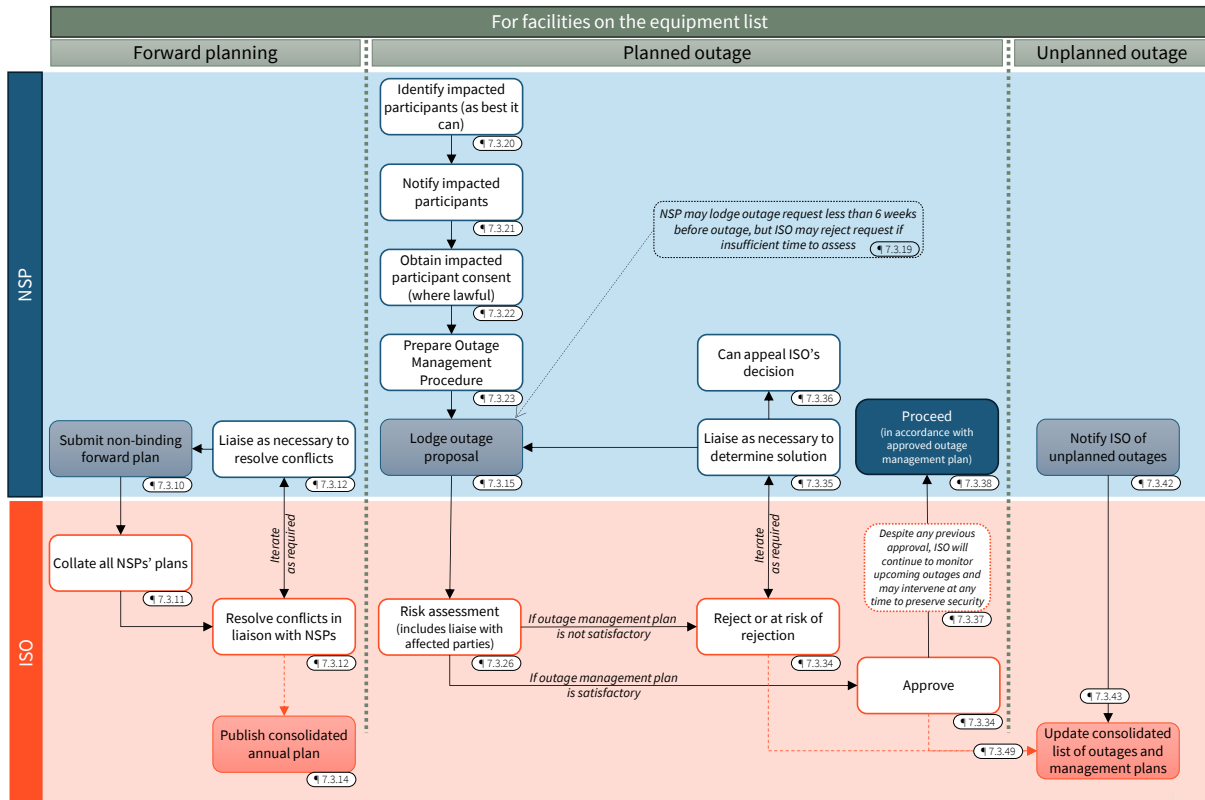


Figure 4 - Proposed Pilbara outage management process

Equipment list

- 7.3.3 The ISO will develop and publish an “**equipment list**” which includes (at least) all significant energy producing facilities, all facilities which provide ESS, and all transmission network elements that serve them.
- 7.3.4 There will be a mechanism (in the WEM Rules it is appeal to the ERA) for a participant to object to its equipment being included on the list.
- 7.3.5 **The following outage management process only applies to equipment on the list.**
- 7.3.6 The test for what gets included in the equipment list should be able to deal with situations like Case Study 4 (section 3.5), in which a piece of equipment within a facility could represent a single point of failure which could take the entire facility offline. However, it should do so in a way which does not require facility operators to provide a full component list, or to undergo the outage management process for every maintenance task.

Integrated mining networks and Pluto facility

- 7.3.7 The exact treatment of integrated mining networks and the Pluto facility will be worked out during the detailed design of the new regime, but the ISO does not propose to depart from the principles set out in paragraphs 7.3.8 and 7.3.9 below.
- 7.3.8 For an integrated mining network, PNR rule 5 will govern how the outage regime applies. This will include which equipment on an integrated mining network is to be listed on the equipment list, and

which directions can be given. The Outage Management Procedure will specify the framework or triggers under which the ISO determines whether a particular event or equipment is to be brought within this outage regime, and a dispute resolution process should the integrated mining network's NSP disagree with the ISO's determination.

- 7.3.9 For Pluto equipment, the below regime should respect the limitations presently set out in the PNR. At present the ISO expects that Pluto equipment will be eligible to be listed on the equipment list, with the present PNR protections for Pluto reflected in limitations on the directions which may be given.¹¹⁵

Forward planning

- 7.3.10 Each year, any participant (registered NSPs, registered controllers and contracted ESS providers) with listed equipment must submit a non-binding forward plan showing all planned outages.
- 7.3.11 The ISO will collate these plans. It may, but is not obliged to, undertake preliminary risk assessment and modelling at this stage, or it may choose to wait until an outage proposal is lodged. The ISO will likely administer a central database for scheduling notifiable events, most of which should be public.¹¹⁶
- 7.3.12 If the ISO identifies scheduling conflicts or risks,¹¹⁷ the ISO will notify the relevant participants and liaise with them with a view to resolving the matter. Participants may update their forward plans as required.
- 7.3.13 The forward plan is non-binding. A participant is not obliged to proceed with outages on the plan, and is free to propose outages which are not included on the plan. However, when it comes to scheduling clashes between proposed outages, outages which have been foreshadowed in a forward plan will have an advantage over those which have not (see para 7.3.33 below).
- 7.3.14 The ISO will compile all participant's forward plans into a single consolidated annual plan, which the ISO will publish. The ISO may update this annual plan from time to time.

Outage proposals

- 7.3.15 If equipment is on the equipment list, then for each notifiable event the relevant participant ("**proponent**") must lodge an **outage proposal** with the ISO. A proponent who is not a registered NSP may appoint its NSP to undertake and manage this process on the proponent's behalf.
- 7.3.16 The outage proposal must include a proposed **outage management plan** describing how the NSP proposes for the risks associated with the event to be mitigated.

¹¹⁵ The PNR regime for Pluto does not presently contemplate the proposed new regime for outage management, dealing only with (relevantly) directions under rule 182(3) to resolve scheduling conflicts because these are the only outage-management directions presently available. Given that the ISO is in this draft decision proposing a materially broader scope of possible directions related to outage management, it will be necessary to determine precisely how Pluto should be treated. This can be developed during the detailed drafting of the rule changes.

¹¹⁶ See for example AEMO's NEM [Network Outage Schedule](#).

¹¹⁷ Some risks will not become apparent without modelling, which may not be justified at this early stage.

- 7.3.17 The notifiable event cannot proceed until the ISO has approved the outage proposal.¹¹⁸
- 7.3.18 The proponent can revise the outage proposal at any time before it's approved. After it's approved, changes will need the ISO's consent.¹¹⁹
- 7.3.19 Outage proposals (or amendments) should be lodged at least 6 weeks before the proposed event. The proponent may lodge a proposal or amendment after this deadline, but the ISO may reject it if it considers that there is insufficient time to properly assess and manage it.
- 7.3.20 The proponent must (to the extent it is able, lacking the full system model) identify all "**impacted participants**", being those people with equipment on the equipment list who will be materially impacted by the outage. The Outage Management Procedure will specify the criteria for determining who is materially impacted.¹²⁰ This may include specifying the classes of participant who can qualify as impacted.¹²¹
- 7.3.21 The proponent must give the identified impacted participants at least 3 months' notice of the outage unless they agree to a shorter period, and must take their views into account in developing its outage proposal and the accompanying outage management plan.
- 7.3.22 To the extent the proponent can lawfully do so, it must endeavour to obtain all impacted participants' agreement to the proposal.¹²² On the other hand, the proponent may ask the ISO to manage this: see paragraph 7.3.31.
- 7.3.23 The Outage Management Procedure will detail what must be included in an outage proposal, but it will include at least:
- (a) details of the planned event including start and end times;
 - (b) the NSP's own risk assessment for the outage (under Draft Recommendation 11 the ISO will develop and publish a standard risk assessment methodology, to be used by all participants for this purpose);
 - (c) an **outage management plan** describing how the NSP proposes for the risks associated with the event to be mitigated;
 - (d) any restrictions on recall;

¹¹⁸ Some regimes provide for deemed approval, if the ISO does not respond in a specified time (e.g. WEM Rules clause 3.18E.4). Deeming approval or rejection can sometimes create perverse incentives for how proponents manage the timeline. This will be considered during the Procedure's detailed design.

¹¹⁹ The regime will likely allow certain changes without consent, e.g. if the change simply makes the outage shorter while still keeping it within the same time window, i.e. starting later or finishing earlier.

¹²⁰ Care, and likely some detail, will be needed to precisely define when a participant qualifies as "impacted" and so becomes entitled to ask the ISO to intervene, and the criteria may need to evolve with experience and as the network transitions. Because of this, we propose to leave this task to the Procedure. This is the approach adopted by the WEM Rules: sections 3.18C.1 and 3.18.4(d).

¹²¹ For example in the WEM Rules, loads cannot be "impacted participants" and so do not qualify for consultation. The detailed procedure development process can determine whether this is or is not an appropriate restriction for the Pilbara, especially for large loads for whom the consequences of an outage may be substantial.

¹²² To reflect the principle in Draft Recommendation 1 that the regime should not require participants to reach agreements which may create competition law risk, this stops short of the WEM Rules, in which the NSP has an unqualified obligation to seek agreement from each impacted participant: WEMR 3.18C.2(b).

- (e) a list of the impacted participants it has identified (see para 7.3.20), confirmation that they have all have been notified, and whether they have all agreed¹²³ to the outage management plan.

Assessment

- 7.3.24 The ISO will assess each outage proposal as quickly as practicable. It will usually assess proposals in the order they are lodged.
- 7.3.25 The ISO may model the proposed event together with any other proposed events, and may consult with other affected parties as it sees fit. It may assess multiple outage proposals as a group.
- 7.3.26 The ISO will make a risk assessment of the outage proposal. The ISO proposes that the **"evaluation criterion"** be:

whether there will be sufficient network and generation capacity in service to maintain security and reliability in affected parts of the network to at least the level they normally were shortly before the outage.

- 7.3.27 The ISO invites feedback on this proposal. To accommodate the reality that different parts of the NWIS presently in practice experience different levels of security and reliability and may be covered by different network planning criteria, this criterion does not refer to a single reliability standard, but rather references the normally-prevailing level of security and reliability in the relevant part of the network.
- 7.3.28 The Outage Management Procedure may set out methods and criteria for the evaluation.
- 7.3.29 The ISO may still approve an outage if this criterion is not met, if the risk associated with not performing the outage is greater.

Coordination

- 7.3.30 In addition to any impacted participants identified by the proponent in its proposal (paragraph 7.3.20), the ISO may identify and notify other impacted participants.
- 7.3.31 Any proponent or impacted participant can ask ISO to help coordinate between the proponent and impacted participants regarding when the proposed outage is to be scheduled, and on what conditions including which mitigations should be implemented.
- 7.3.32 ISO will liaise as necessary and can if necessary direct a resolution, and the outage proposal and outage management plan will be updated accordingly.
- 7.3.33 The rules or procedure will specify the criteria to be applied in this coordination process but, subject always to maintaining security and reliability, a notifiable event disclosed in an annual plan will

¹²³ As discussed in footnote 122, the regime will permit, but not require, the proponent to discuss and agree outage mitigation measures with other participants.

generally take priority over one which is not, and outage proposals will generally have priority from the time of lodgement.

Approval

- 7.3.34 After the assessment and any coordination, the ISO will publish its conclusions on the outage proposal (approved, rejected, or at risk of rejection).¹²⁴
- 7.3.35 If the ISO rejects a proposal or classifies it as being at risk of rejection, the proponent may liaise with the ISO and (subject to the time limits above) may amend its proposal until it has remedied the problem to the ISO's satisfaction. For example, this may involve more or different mitigations or different recall arrangements.
- 7.3.36 If ISO rejects a plan, the proponent can appeal this (probably to the ERA).
- 7.3.37 Once an outage has been approved, the ISO can reject (un-approve) it if there has been a change in power system conditions such that the evaluation criterion is no longer satisfied or the risks have otherwise become unacceptable.

The outage

- 7.3.38 The proponent may proceed with an approved outage, and in doing so must comply with the approved outage management plan including:
- (a) implementing any mitigations specified in the plan;
 - (b) (if specified in the approved outage management plan) obtaining ISO control desk consent before starting the event or before returning the equipment to service;
 - (c) ensuring the equipment is returned to service within the allotted time;
 - (d) complying with any recall obligations.
- 7.3.39 However PNR rule 172 (Grounds for non-compliance, i.e. safety etc) will apply to this obligation.

Recall

- 7.3.40 The outage management plan may specify circumstances in which the ISO or ISO control desk may recall equipment to service.¹²⁵
- 7.3.41 In any event the ISO can always recall equipment from outage if necessary for power system security or reliability (subject to GEIP and PNR rule 172).

¹²⁴ During detailed design, the ISO will consider whether to adapt the NEM terminology described in paragraph 7.2.11.

¹²⁵ The Protocol Framework Procedure already provides for recall during a contingency, and will likely need some adjustment to integrate with this.

Unplanned outages

7.3.42 As now, a registered NSP or registered controller must notify the ISO and ISO control desk of any unscheduled notifiable event which might impact security, reliability, provision of ESS or access services on a covered transmission network.

7.3.43 The ISO will publish this information.

Commissioning and testing

7.3.44 A procedure or the rules will specify the circumstances in which commissioning or testing *must* occur, e.g. after major maintenance, to test control systems, to qualify to provide ESS, significant new connections, etc. This will not limit the circumstances in which a proponent may otherwise elect to put forward a commissioning/testing proposal.

7.3.45 Commissioning and testing will be dealt with in the same way as outages, e.g.:

- (a) the proponent must put forward a proposal which includes a commissioning/testing plan;
- (b) impacted participants must have been notified in time;
- (c) commissioning/testing cannot proceed until the ISO has approved the plan;
- (d) the ISO can suspend commissioning/testing on the same rules as apply to outage recall.

7.3.46 The ISO must endeavour to accommodate the proponent's reasonable needs in relation to commissioning or testing, unless this would jeopardise security or reliability.

7.3.47 The procedure may provide different timelines for commissioning/testing than for other notifiable events, and may allow greater flexibility on these timelines.

7.3.48 ISO will publish basic details of each approved commissioning/testing plan.

Transparency

7.3.49 For each outage proposal the ISO will publish:

- (a) a description of the outage including the equipment impacted;
- (b) the proposed outage start time and duration;
- (c) the status of the outage (approved, rejected, at risk or rejection);
- (d) the outage proposal first submission date;
- (e) at least summary details of the outage management plan;

7.3.50 The ISO will publish comparable details for each commissioning/testing proposal.

7.3.51 The ISO will publish rejections, recalls and unscheduled outages.

7.3.52 During detailed drafting, these transparency measures should be reviewed as described in Draft Recommendation 2 above, to determine whether any exceptions for commercially sensitive information must be included, and if so how those exceptions might be minimised in order to maximise transparency.

7.4 How the section 7.3 process might be implemented

7.4.1 The ISO proposes to split the details of the above process between rules and the procedure, in order to create a fair balance between certainty and flexibility.

7.4.2 The detail of this split will emerge during the detailed drafting of rule and procedure change proposals. As noted in para 6.6.5 above, the SWIS regime can be a guide as to the split, although the NWIS regime is less complex.

7.4.3 Both rules and procedures should allow for some flexibility, to accommodate:

- (a) refinements or corrections which emerge as the regime is operated in practice; and
- (b) the continued evolution and growth of the Pilbara electricity marketplace.

7.5 How the section 7.3 process would have dealt with the four case studies in section 3

7.5.1 In **Case Study 1** (see section 3.2) there was disagreement as to whether the loss of a particular line was a credible risk, and hence whether a machine start was necessary. The above process would have:

- (a) required both NSP A and NSP B to adopt a common risk assessment framework, which would hopefully reduce the risk of disagreement on fundamental questions such as the likelihood of loss of the line in question;
- (b) if the NSPs still disagreed, allowed the ISO to make the final determination on the question;
- (c) enabled the ISO adequate time to model the outage and its attendant risks, to determine whether a machine start was necessary, or whether some other (if any) mitigation measure might be more appropriate;
- (d) assuming a machine start remained the preferred solution, enabled the ISO or ISO control desk to direct the relevant machine to start (see section 8.2), thus ensuring that the generator in question could access the cost-allocation methodology to be determined by a broader review (see section 8.3, and see also section 8.5 on the possible use of ESS for this purpose).

7.5.2 In **Case Study 2** (see section 3.3), it's to be hoped that a common risk assessment framework would avoid an outcome in which one NSP classified as minor a consequence which the other NSP classified as extreme. In any event, the ISO's role as final arbiter on risk mitigation measures would have enabled the controversy to be resolved definitively one way or the other. Because the ISO holds the

whole of system model, it will likely be in a better position that the proponent to assess risks in other networks.

- 7.5.3 In **Case Study 3** (see section 3.4), the pre-approved outage mitigation plan would have shown the role of the black start machine in managing risk. If the black start machine's outage was planned or foreseeable, it may have been reported in sufficient time to allow the outage in question to be rescheduled, or other mitigation measures put in place. Or, if the black start machine's outage was unscheduled, the ISO control desk would have had the power to cancel or recall the scheduled outage due to the changed circumstances.
- 7.5.4 In **Case Study 4** (see section 3.5) having the outage raised and assessed in adequate time would likely have avoided the NSP's mistaken advice, and would in any event have enabled the ISO to properly assess the system risk associated with the relevant device running on an N-0 basis for the week in question. Further, if the matter did remain unresolved before the outage was due to start, the NSP would not have been able to just go ahead with the outage despite the ISO's concerns.

8. Mitigation of outages*

8.1 Introduction

- 8.1.1 One of the main areas of controversy over the last 12-18 months has been the measures to be put in place to mitigate the risk associated with planned outages. Specifically, for a given outage:
- (a) Are mitigation measures necessary?
 - (b) What form should they take and who should undertake them? and, of course
 - (c) Who should pay?
- 8.1.2 These controversies have been exacerbated by several factors: the participants have not been using a common risk assessment framework; the matters are often being discussed at the last minute and in the absence of proper modelling; and (the subject of this section) there has been disagreement about who has powers to make the necessary determinations.

8.2 Who determines which mitigations should be implemented?

- 8.2.1 The ISO proposes that it should be the final arbiter of what mitigation or other risk management measures are required for any given notifiable event.
- 8.2.2 The mechanism will be through the ISO's approval of the outage management plan (see section 7.3), including its ability to not approve the plan until it has been amended to the ISO's satisfaction (e.g. to include additional or different mitigations).
- 8.2.3 In making its decision to approve or not approve an outage proposal (and the outage management plan it contains), the ISO will undertake modelling and other investigations as it deems fit. This will include any consultations the ISO deems appropriate.
- 8.2.4 The ISO will be assisted in this exercise by the fact that the proponent is required to have already, to the extent it is able, have identified and notified impacted participants.
- 8.2.5 The ISO will have time to undertake this evaluation and consultation, because the outage proposal will have been lodged at least 6 weeks before the outage start date. (It may be lodged later than this deadline, but the ISO may reject it if that leaves it insufficient time to assess the proposal properly.)
- 8.2.6 Hopefully, many of the outages will have been notified up to a year ahead through the non-binding annual plan mechanism, allowing plenty of time for modelling, discussion of options, etc.

Draft Recommendation 15: The ISO, through its power to approve or reject proposals for notifiable events, will be responsible for determining which mitigations or other management measures should be implemented for an event.

* *Reminder: References to outages in this draft decision generally include all notifiable events. See section 1.4.*

8.3 Who is responsible for implementing mitigations?

- 8.3.1 Sometimes, the necessary mitigation will require action by the proponent of the outage proposal. In this instance, the requirement that the proponent comply with the outage management plan (paragraph 7.3.38) will ensure that the required mitigation is implemented.
- 8.3.2 But on other occasions, the optimum mitigation will require action by a third party. For example in Case Study 1 (see section 3.2), the proponent of the outage proposal would have been NSP A. If the ISO determined that the loss of the relevant line was a credible risk, and agreed with NSP B that the appropriate mitigation was to start a machine within the relevant zone whenever its load appeared likely to exceed 25 MW, then it would be necessary to place an obligation on the controller of that generator to start a machine whenever load was approaching that threshold.
- 8.3.3 This would require the ISO or ISO control desk to have the power to direct that person to start a machine.¹²⁶

Draft Recommendation 16: That the ISO be empowered to direct the proponent, and if appropriate other participants, to take measures to mitigate notifiable events. That the ISO control desk have the power to activate these measures as necessary during real-time operations.

8.4 Dealing with the costs of mitigation

- 8.4.1 If a person is required to take measures to mitigate an outage, such as starting a machine, reducing demand or rebalancing load between generators, and those measures have a cost, the regime should deal with the question of who bears that cost.
- 8.4.2 This raises larger policy issues, which are best dealt with by a broader review.
- 8.4.3 For the present, the ISO simply makes the following high-level observations:
- (a) It is not good policy for the question of who should bear the mitigation costs to be answered by default, by letting them simply lie where they fall. Perhaps the person who incurs the costs is indeed the best person to bear them, but this should be a conscious policy outcome.
 - (b) If outage mitigation requires machine starts or other activity which overlaps with the services provided by an ESS provider, the question of who should bear the costs of the outage mitigation should be answered separately. The normal ESS cost allocation mechanism may or may not produce the best answer (see also section 8.5 below). Once again, this question should not be left to be answered by default.
 - (c) There is a policy decision to be made as to whether cost allocation should be causer pays, beneficiary pays (and if so, how the beneficiaries are to be determined), or socialised in some way on the basis that security and reliability benefit all users. There is no obvious answer to

¹²⁶ The precise mechanism for this can be developed during the detailed rule drafting stage. For example, this could be done by way of a standalone direction, or by way of a rule which permits approved outage management plans to place obligations on third parties. Safeguards would be needed in either case, such as making sure the third party was appropriately consulted, was in a position to comply, etc.

this, and it's quite possible that the fairest answer will change depending on the circumstances.

- (d) It may also sometimes be necessary to identify which actions are genuinely costs of mitigating an outage, and which actions might have been undertaken anyway for some other reason, because arguably only the former costs should be recovered through any outage cost allocation mechanism.
- (e) In a similar vein, presumably only efficient costs should be compensated.
- (f) Care will be needed to ensure there are not perverse outcomes, e.g. proponents deferring maintenance outages to avoid the cost of mitigation, or participants manipulating their operations so that they can get paid to do something (e.g. starting a machine) they would have done anyway.

Draft Recommendation 17: That a broader review address the question of how notifiable event mitigation costs should be identified, assessed and allocated.

8.4.4 It is likely that one or more existing Procedures may need adjustment, after these matters are resolved. This will be addressed in due course.

8.5 Use of ESS to mitigate outages*

8.5.1 An issue has emerged as to whether the ISO can or should use ESS to mitigate outage risks and, if it does, whether it's appropriate to recover the associated costs through the existing cost allocation methods in PNR Subchapter 8.3.

8.5.2 For example in Case Study 1, during an extended outage in network A the remaining network configuration to serve a zone in network B consists of two lines (lines B1 and B2), of which one (line B2) has a thermal limit of 25 MW. As such, during the outage, whenever the load in that zone exceeds 25 MW, the zone in effect faces N-0 reliance on a single line (line B1).¹²⁷ The NSP for network B wishes to start a machine in this zone whenever necessary to ensure that the zone's imports remain below 25 MW, but cannot secure a consensus between NSPs on whether this is necessary. In the absence of a consensus, the NSP proposes that the ISO should use an SRESS service for this purpose, specifically a 'Supplemental SRESS' such as the ISO proposed to procure earlier this year.¹²⁸ The NSP contends that the associated cost should be allocated under the usual SRESS formula in rule 229.

8.5.3 This approach would have some attractions:

- (a) ESS procurement and activation is an established mechanism under the rules;
- (b) the PNR do provide at least some link between outage management and ESS, because one of the "system coordination matters" to be discussed under Subchapters 7.3 and 7.4 is any

* *Reminder: References to outages in this draft decision generally include all notifiable events. See section 1.4.*

¹²⁷ See more complete description in section 3.2 above.

¹²⁸ ISO, *Final Determination: Flexible approach to Spinning Reserve Essential System Services*, May 2024 (available [here](#)).

necessary or desirable measures to manage the power system during the event, “including any changes in essential system service procurement, configuration, enablement or dispatch”;¹²⁹

- (c) the load-based machine start service required in Case Study 1 is in some ways similar to the (yet to be tested or implemented) headroom-based “dynamic enablement” SRESS model anticipated by PNR rule 216;
- (d) this approach could perhaps be accommodated within a suitably sophisticated flexible determination methodology for the “required headroom level” under PNR rule 212(1)(b), if appropriate risk assessment and modelling could be done (but see the countervailing view in para 8.5.6 below); and
- (e) importantly, it would provide a payment mechanism for the machine being started—something which is clearly missing under the present regime.

8.5.4 But at present the ISO is not confident that the PNR permit this approach.

8.5.5 Some of the difficulties lie in Subchapters 7.3 and 7.4. The outage regime in these Subchapters was deliberately designed to be led by the NSPs, not the ISO, whose role is largely limited to coordination and advice. Not only does the ISO have no general *dispute resolution* role under these Subchapters (outside scheduling conflicts), but in fact the PNR state explicitly that it does not even have a general obligation even to *investigate* notifiable events.¹³⁰ In circumstances where the NSPs have been unable to agree on whether the loss of line B1 is a credible contingency, and as a result have been unable to agree on whether mitigation measures are needed let alone how they should be paid for, the present rules provide no clear role for the ISO to intervene and impose its own solution on the parties. Nor does the current process have any clear mechanism for the ISO to undertake the risk assessment required to establish the decision parameters the ISO control desk would need, in deciding whether and when to enable machines to mitigate a given outage.

8.5.6 Other difficulties lie outside Subchapters 7.3 and 7.4. In Chapter 8, SRESS procurement and enablement is underpinned by the concept of an ISO-determined “required headroom level”. There’s little to suggest that this concept was intended to be used on an ad hoc basis to mitigate outages, or how such determination should integrate with the outage management process in Subchapters 7.3 and 7.4.

8.5.7 Also, if SRESS was being used to mitigate outage risk, it is not clear whether the ‘runway’ model for cost allocation in rule 229 would produce a sensible or fair outcome, in terms of either the payers it selects, or how it shares costs between them. Certainly, rule 229 was not designed with outage mitigation in mind.

8.5.8 There are also other drafting difficulties in how outage mitigation might fit into both Subchapter 7.5 and Chapter 8.

¹²⁹ PNR rule 167(c)(iii), noting however that outside scheduling conflicts, the ISO has no unilateral power to impose its own determinations regarding system coordination matters.

¹³⁰ PNR rule 177(4)

- 8.5.9 In short, under the rules as presently drafted the ISO is not convinced that, in a situation such as Case Study 1, it can or should intervene to use ESS to impose unilaterally a solution on NSPs who have failed to reach consensus, and to impose costs on ESS payers.
- 8.5.10 This produces an unacceptable outcome. If, after a suitable risk assessment, it is determined that a machine needs to be started out of merit to properly mitigate the risks associated with an outage, then the ISO control desk needs a clear authority to direct the machine to start, and the machine's operator should get paid for the marginal costs of complying.¹³¹ But for this to happen the ISO control desk must have suitable decision criteria on when to issue such a direction, and those criteria must be supported by an appropriate risk assessment.
- 8.5.11 The recommendations set out elsewhere in this draft decision should equip the ISO and ISO control desk with the process, time and powers to undertake the necessary risk assessment, and the approved outage management plan for an outage should set out the correct decision criteria for when the ISO control desk may issue a direction to start a machine. What remains is to consider whether contracted ESS can and should be used for this purpose. Further, if ESS is used, are the cost allocation mechanisms currently in Subchapter 8.3 appropriate for this use of ESS? These are subjects on which the ISO invites stakeholder feedback.
- 8.5.12 At present the ISO is inclined to the view that if outage mitigation requires a particular machine to be started, and the ISO has an ESS contract in place with the relevant generator which permits the ISO to direct the generator to start that machine, then it may be that ESS is a useful tool for this purpose, and if so the rules should empower the ISO to use its ESS contracts for the purpose. Pending any other suitable ESS arrangements,¹³² the rules could permit the ISO to use Supplementary SRESS for this.
- 8.5.13 In terms of cost allocation, the ISO proposes that until a broader review determines a more appropriate cost allocation methodology (see Draft Recommendation 17), the cost of these machine starts should be distributed under the existing Subchapter 8.3 mechanisms. Hence, if SRESS is used, for the time being the cost will be distributed through the runway model in rule 229.

Draft Recommendation 18: That during the detailed design of the new regime, consideration be given to whether the ISO should be permitted to utilise ESS contracts to manage notifiable events, and if so in what circumstances. Further, if so, that the review under Draft Recommendation 17 determine how the resulting ESS costs should be allocated.

- 8.5.14 Finally, the use of ESS could provide a useful interim solution, pending more comprehensive changes to the outage management regime discussed elsewhere in this draft decision. Even if imperfect, a power to use ESS would at least address the ISO's present lack of any other clear power to direct machine starts for outage mitigation. Only modest changes would be needed to Subchapters 7.3 and

¹³¹ This proposition stands even though, where the generator in question is vertically integrated, sometimes the appropriate 'payer' may be its own related network business. The point is that the rules should address who is to pay, not simply leave the costs lying on the generator by default.

¹³² It has been suggested that Supplementary SRESS is a suitable service. It is possible to construct an argument that machine starts discussed in Case Study 1 constitute a form of SRESS, but this argument has at least two difficulties. The first is that most of the language in Chapter 8 discusses SRESS and its related concept of headroom on a system-wide or island-wide basis. It's perhaps arguable, but not clear, that SRESS can also be used on a non-island subset of the NWIS. The second is the machine starts in Case Study 1 might be better described as a network support service, reducing load in a zone to prevent network overload.

7.4, Chapter 8 and the relevant Procedures to allow ESS to be used in this fashion. The ISO therefore seeks stakeholder feedback on whether it should progress urgent interim rule and procedure changes to activate this measure:

Draft Recommendation 19: That the ISO propose urgent rule and procedure changes as necessary, to enable it to use ESS to mitigate notifiable events, as an interim solution pending any more complete rule changes which may be developed following this review and any broader review. Further, that pending a suitable answer to the question of how mitigation costs should be identified, assessed and allocated, the costs of ESS contracts used in this fashion should be recovered through standard Subchapter 8.3 processes.

9. Matters left for a broader review

9.1.1 The following matters were identified during this review or raised by stakeholders, but affect more than just the Subchapter 7.3 and 7.4 processes. These matters should be addressed by other processes in due course:

- (a) Pilbara ISOC Co Ltd's membership, internal governance and funding;
- (b) PNR governance generally;
- (c) NSP vertical integration;
- (d) the ISO's delegation of the control desk function to Horizon Power¹³³ and Horizon Power's internal governance regarding that function (except as discussed in section 6.3 above);
- (e) the regime's emphasis on NSP autonomy and reliance on informality and collaboration, elsewhere than in Subchapters 7.3 and 7.4;
- (f) the interaction between outages and how system operating states are defined, and when and how the ISO's and ISO control desk's powers are or are not activated under rules 185, 186 and 187, including the overlapping definitions of "notifiable event", "contingency" and "pre-contingent threat";¹³⁴
- (g) the specification, procurement and enablement of, and cost recovery for, essential system services (**ESS**) under Chapter 8 of the rules (except as discussed in section 8.5 above);
- (h) the role of network planning criteria;¹³⁵
- (i) the binary definition of "island";¹³⁶
- (j) whether the definition of "system security objective" needs attention;¹³⁷
- (k) how outage assessment should interact with constraint management.¹³⁸

Draft Recommendation 20: That in due course a broader review should address the matters identified in this section 9.

¹³³ The rules permit, but do not require, the ISO to delegate the control desk function: rule 45.

¹³⁴ Issues Paper section 5.3

¹³⁵ Issues Paper section 6.1

¹³⁶ See section 5.4 above.

¹³⁷ See footnote 50 above.

¹³⁸ See para 7.2.16 above.

Appendix 1: Stakeholder Feedback on Issues Paper

Following publication of the Issues Paper, the ISO conducted face-to face meetings with market participants, and received written submissions.

The meetings and submissions were informal and confidential, and for the purposes of PNR rule 299 the ISO does not consider it necessary to disclose which stakeholders provided feedback on which subjects.

However in the interests of transparency, the ISO sets out below a high-level summary of some of the major points made by stakeholders during this feedback, together with the ISO’s response. **This table does not attempt to be completely exhaustive. If you raised an issue which you feel is not adequately addressed below, you are welcome to raise it again in your submission on this draft decision.**

Feedback on Issues Paper	ISO response
General	
<p>1. Some stakeholders felt that no or few rule changes were necessary, and no new procedure was necessary. The present approach which grants NSPs a high degree of autonomy, subject only to collaborative fortnightly meetings, was working sufficiently well.</p>	<p>The Case Studies set out in section 3 illustrate why the ISO does not support the status quo.</p> <p>Creating a formal outage management process need not eliminate informal collaboration. The presence of an authorised decision-maker with clear powers to resolve disagreements may in fact make impasses less likely.</p>
<p>2. Some stakeholders put a variation on this submission: that although the current regime may not be working effectively, there is sufficient scope within the current rules to change participants’ behaviour to better manage outages, without needing rule changes, for example by scheduling a series of additional extraordinary system coordination meetings to pre-agree solutions for likely future outage scenarios.</p> <p>(These submissions generally rely on one or more of the legal interpretations set out in row 48 onwards, below.)</p>	<p>The ISO disagrees. It considers that the current rules lack suitably clear objectives, functions and powers.</p> <p>It considers that the improved process should be transparently documented in the rules and a procedure, and that its outworkings should also be clearly documented and wherever possible transparently available to all participants.</p>
<p>3. Some stakeholders praised the current regime’s low compliance burden.</p>	<p>The ISO will be mindful of the compliance burden when designing the new regime.</p> <p>The ISO also notes that on the flipside of the coin, others criticised the current regime’s opacity.</p>
<p>4. A stakeholder said that if this review resulted in proposals to change the rules, that would decrease certainty and hence be a barrier to new investment in renewable energy.</p>	<p>This is a matter to be considered in the coming rule change process, but the ISO observes that although stability in rules can be a good thing, it may not always be, e.g. if the current rules are inadequate.</p> <p>New investment in renewable energy is not likely to be fostered by leaving in place poor processes which are opaque, favour certain incumbents and are inadequate to manage system risk.</p>
<p>5. Conversely to rows 1 to 4, some stakeholders said that change was necessary, because the current reliance on informal discussions at the system coordination meetings and informal assessment and approval by the ISO and ISO control desk were unsatisfactory.</p>	<p>The ISO agrees.</p>

<p>6. However, one of the stakeholders who advocated for change did caution that the impact of a more formal process on timely approvals should be thoroughly understood.</p>	<p>The proposed new process is designed to allow up to a year for outages to be assessed and resolved.</p>
<p>7. Some stakeholders asked that rule changes be minimised wherever possible.</p>	<p>The ISO agrees with this as a general principle, but nonetheless intends to propose substantial changes following this review. Minor tweaking will not be adequate.</p>
<p>Overarching objective</p>	
<p>8. Several stakeholders encouraged the ISO to build the risk assessment framework around a single clear objective, focussed on security and reliability of supply.</p>	<p>The ISO agrees. Draft Recommendation 7 is to focus Subchapters 7.3 and 7.4 on the system security objective.</p>
<p>9. A stakeholder considered that transparency about outages is the most important driver of efficiency and reliability.</p>	<p>The ISO agrees. See comments on the EU REMIT scheme discussed in section 7.2 above.</p>
<p>Definitions</p>	
<p>10. Three stakeholders supported the breadth of the current definition of “notifiable event”.</p> <p>One of them supported correcting the ambiguity in rule 186(1), discussed in footnote 47 above.</p>	<p>The ISO agrees. See Draft Recommendations 3, 4 and 5.</p>
<p>Roles and responsibilities</p>	
<p>11. There was general but not universal stakeholder support for the ISO to have the central risk assessment function, including resolving disagreements between NSPs or other outage proponents.</p>	<p>This is included in the proposed new outage management procedure in section 7.3 and Draft Recommendation 14 (“proposed new process”).¹³⁹</p>
<p>12. Some stakeholders acknowledged that this will require the ISO to be resourced for this function.</p>	<p>See Draft Recommendation 9.</p>
<p>13. There was also general support for the ISO to have the central outage modelling function, and for the proposed new process to require outage proposals to be lodged sufficiently far in advance to allow time for this to occur.</p>	<p>The proposed new process provides for this.</p>
<p>14. Several stakeholders agreed that the ISO should have powers of direction regarding outages.</p>	<p>The ISO agrees. See Draft Recommendation 12.</p>
<p>15. Some stakeholders supported the creation of a new Outage Management Procedure.</p>	<p>The ISO agrees. See Draft Recommendation 13.</p>
<p>16. Another stakeholder considered that no new Procedure is required, because the ability to establish alternative arrangements for system coordination meetings is sufficient.</p>	<p>The ISO does not consider the system coordination meeting approach to be adequate. It will be replaced by the proposed new process.</p>

¹³⁹ Subject to PNR rule 5, for an integrated mining network.

<p>17. Stakeholders generally supported the ISO’s proposal to remove the ISO control desk from its present de facto role in outage assessment and planning. Some stakeholders observed that this practice has led to some confusion about roles and responsibilities.</p>	<p>The ISO proposes to do this, see Draft Recommendation 10.</p>
<p>18. Some stakeholders observed that having Horizon Power operate the control desk creates uncertainty – if a message is received from the control desk, it’s unclear whether it comes from the ISO’s delegate, or from the NSP.</p> <p>Another stakeholder pointed out the control desk’s conflict of interest.</p>	<p>The ISO acknowledges this feedback, but considers Horizon Power’s vertical integration to be a matter for a broader review.</p>
<p>19. A stakeholder suggested that a least cost way for the ISO to fulfil the new roles being proposed would be to outsource the modelling and risk assessment.</p>	<p>See Draft Recommendation 9. The ISO will seek to implement the most efficient mix of insourcing and outsourcing.</p>
<p>20. A stakeholder suggested that there should be clear terms of reference for system coordination meetings.</p>	<p>The system coordination meetings will be replaced by the proposed new process.</p>
<p>21. Some stakeholders sought confirmation that the existing rules regarding Rio Tinto’s network and the Pluto facility would be preserved.</p>	<p>This is what the ISO proposes, see paras 7.3.8 and 7.3.9 above.</p> <p>The precise outworking of this will be a matter for detailed rule and procedure development following this review.</p>
<p>Process and timing</p>	
<p>22. Some stakeholders said that the WEM Rules process should not be used as a template because it is too prescriptive and too complex. For example it includes features designed to support the WEM capacity market.</p>	<p>The proposed new process is simpler than the WEM Rules’.</p>
<p>23. Some stakeholders observed that the Pilbara regime will need to address aspects not present in the WEM, such as multiple NSPs and a regime for pre-contingent threats.</p>	<p>The ISO agrees. See the proposed new process.</p>
<p>24. A stakeholder said that informality and imprecision of the system coordination meeting was a problem.</p>	<p>The ISO agrees. The proposed new process is designed to remedy this.</p>
<p>25. Some stakeholders said that the outage management process should culminate in clear instructions to the ISO control desk on how to manage an outage.</p>	<p>The ISO agrees. The outage management plan produced by the proposed new process is intended to deliver this.</p>
<p>26. Numerous stakeholders agreed that discussing outages much earlier (e.g. > 6 months before the outage) would allow more time for risk assessment and selection of mitigation measures, and more time for disagreements to be resolved.</p>	<p>The ISO agrees. The proposed new process is designed to deliver this.</p>
<p>27. Some stakeholders observed that the network configuration was so simple that it should be possible to pre-agree risk assessments and mitigation measures for the small number of network elements (some suggested less than 5) on which outages could involve material risk.</p>	<p>The ISO is not sure that the number of permutations is quite that small, but agrees that it should be possible to have a pre-agreed playbook for many of the most significant or recurring outages. This can be developed under the new Outage Management Procedure.</p>

<p>28. A stakeholder suggested that the ISO should not have a general outage approval function, but rather should intervene on an exceptions basis.</p>	<p>The ISO considers that the important thing is to ensure that outages undergo a proper, timely, central and transparent risk assessment. The fine detail of the new process remains to be developed.</p> <p>During that stage the ISO will be open to considering whether the process can work effectively on an exceptions basis. At present, however, its proposal is for all outages of listed equipment to require approval. For minor, routine or low-risk outages, this approval may be able to be given very quickly.</p>
<p>29. Conversely, another stakeholder suggested that the ISO should have a general approval function for every outage.</p>	<p>This is set out in the proposed new process.</p>
<p>30. A stakeholder discussed the need for there to be a power for last-minute cancellations and recalls, wherever possible exercised by the ISO rather than the ISO control desk.</p>	<p>The ISO agrees. The proposed new process is designed to deliver this.</p> <p>At some point approaching real time the outage needs to be handed over from the ISO to the ISO control desk to manage, but by this stage the instructions to the control desk on how to deal with various eventualities should be clearly set out in the approved outage management plan.</p>
<p>31. A stakeholder observed that the question will rarely be whether an outage should proceed, but rather what controls and mitigations may be needed before it can do so.</p>	<p>The ISO agrees. The proposed new process is designed to get this sorted out well ahead of time, based on a standard risk assessment framework and supported by suitable modelling.</p>
<p>32. A stakeholder observed that the Interim Protocol Framework Procedure may need to be updated to better represent when protocols might be activated.</p> <p>Another stakeholder spoke of the need to cover off the overlap between outage planning and pre-contingent threats.</p>	<p>The ISO agrees. See Draft Recommendation 4.</p>
<p>Risk assessment</p>	
<p>33. There was general stakeholder support for the ISO to develop (i.e. adopt and adapt from elsewhere) a common risk assessment framework for use across all managed outages.</p> <p>One stakeholder explicitly endorsed AEMO's current methodology.</p>	<p>The ISO agrees. See Draft Recommendation 11.¹⁴⁰</p> <p>The methodology to be adopted will be chosen in consultation with affected participants.</p>
<p>34. A stakeholder said that this central risk assessment needs to consider all customers, not just those on a particular network.</p>	<p>The ISO agrees.</p>
<p>35. However, some stakeholders felt that the NSPs should do their own risk assessments using their own frameworks, before handing the results to the ISO for it to assess with its own risk framework.</p>	<p>The proposed new process allows for the outage proponent to put forward its own proposed mitigations. The ISO will assess them.</p> <p>The ISO's outage assessment role will not displace the NSPs general obligations as responsible network operators.</p>

¹⁴⁰ Subject to PNR rule 5, for an integrated mining network.

<p>36. As a related point, a stakeholder said that the outage proponent should not be assessing risks for other people – that should be the ISO’s job. (However, to the extent the proponent had identified a risk, it should share it with the ISO when proposing the outage.)</p>	<p>See row 35.</p> <p>The proposed new process requires the proponent to identify as many impacted persons as possible and to notify them. The ISO may identify and notify others.</p>
<p>37. Some stakeholders said that outage risk assessment and mitigation decisions should primarily be driven by the requirements of system security and reliability, rather than commercial factors (although the cost of mitigation options will still remain a relevant consideration).</p>	<p>The ISO agrees. This will be reflected in the proposed new process.</p>
<p>38. In response to Issue 16 in the Issues Paper, some stakeholders discussed the role of network planning criteria in risk assessment.</p>	<p>The ISO has deferred this matter to a broader review.</p>
<p>Mitigation measures – selecting and directing</p>	
<p>39. Some stakeholders observed that when the ISO presently acts as an informal outage assessor, and presently calls on the ISO control desk for support in this informal role, both the ISO and the ISO control desk are being forced to make decisions about outage mitigation without the benefit of proper modelling. The stakeholder felt that this should be remedied.</p>	<p>The ISO agrees. The proposed new process will allow time for proper risk assessment and modelling to occur, and the change in functions will give the ISO clear authority to undertake the modelling and clear power to make the resulting decisions.</p>
<p>40. Some stakeholders suggested that by the time an outage reaches the ISO control desk for real-time management, there should be a clear outage management plan in place, based on proper modelling, to guide the control desk operators as they manage the system during the outage.</p>	<p>The ISO agrees. The proposed new process provides this.</p>
<p>41. Another stakeholder extended this proposition to management of pre-contingent threats, which could also often have been the subject of prior risk assessment and mitigation selection.</p>	<p>Draft Recommendation 4 calls for the design of the new regime to minimise inconsistencies, overlaps or gaps between outage management, the pre-contingent threat regime, and ESS.</p>
<p>42. A stakeholder said that each NSP proposing an outage should do its own mitigation, and the ISO’s role should be limited to deciding what other mitigation measures may be necessary.</p>	<p>The ISO does not agree with this proposal to split the responsibility. Under the proposed new process, the outage proposal will include the proponent’s plan for how the outage is to be managed which will include the proponents suggestions for mitigation. The ISO will assess this plan, and may approve it or require changes.</p>
<p>43. Some stakeholders discussed the need, when the ISO control desk calls on a generator to start a machine to mitigate an outage risk, for there to be a clear legal framework to govern that request, to clarify the generator’s legal position and entitlement to be paid.</p> <p>A stakeholder observed that the consequences for a generator can extend beyond just additional gas and O&M costs – it may have other obligations under contracts with offtakers.</p> <p>A stakeholder with generating facilities felt that any such request should be the subject of a formal notice or direction under the PNR. Another stakeholder suggested that the request should be governed by a contract put in place with the ISO ahead of time, as with SRESS.</p>	<p>The ISO agrees with the need for a clear legal framework. At present, it feels that this will be more efficiently managed through the rules than a series of negotiated contracts, but notes that EPWA’s PNR Evolution review may also have something to say about this.</p> <p>Section 8.5 discusses the use of ESS in outage management.</p> <p>When detailed rule and procedure proposals are being drafted, incumbent generators should review their offtake contracts for inconsistencies.</p>

44. Some stakeholders discussed the use of ESS contracts to mitigate outage risks, and the EBAS mechanism to distribute the costs.

See discussion in section 8.5.

The ISO proposes that ESS contracts be considered as a potential way to manage outages and their associated costs. See Draft Recommendation 18.

Further, that this might be implemented as an urgent interim measure to fill the current gap in the rules. See Draft Recommendation 19.

Otherwise, the ISO has deferred the role of ESS more broadly to the EPWA PNR Evolution review. EPWA's proposals in this respect may influence how the ISO designs its rule changes after this Subchapter 7.3 and 7.4 review.

Compensation for mitigation actions – payees and payers

45. Some stakeholders said that if a generator was directed to start a machine in order to mitigate an outage risk, it should be reimbursed for the cost.

The ISO agrees. It has deferred to a broader review the question of who pays, recognising that in some permutations the appropriate payer might be the generator's own related NSP business.

46. A stakeholder gave a hypothetical example of the complexities of allocating mitigation costs: Suppose an NSP invests to build an additional network element, improving redundancy in that area of the network from N-0 to N-1, and suppose this reduces ESS requirements and thus saves ESS payers money. Suppose the NSP later wants to take the line out of service for maintenance. Should machine starts or other mitigation be required during the outage, in order to maintain the new N-1 level of redundancy, or is it adequate to allow the system to revert to its previous N-0 level of redundancy during the outage? If a machine start is required, who should pay for it? The NSP who caused the outage, or all the ESS payers who had been benefitting from the new line's ESS savings?

The stakeholder should raise this example with EPWA for consideration while it designs the mitigation cost recovery regime.

See also discussion in section 8.5 above.

As a general principle, the ISO does not consider that historical reliability, before past system upgrades were commissioned, is the appropriate yardstick for outage management. It has proposed that the assessment criterion be to preserve the level of security and reliability normally experienced in the affected part of the NWIS, shortly before the proposed outage (see paragraph 7.3.26) .

47. Views were expressed on whether compensation should be allocated on a causer-pays model or some other model.

Deferred to broader review.

Legal interpretations submitted but not followed

The ISO does not propose to rely on the following stakeholder submissions.

Introduction to rows 48 to 56:

The Issues Paper identified several areas in which, in the ISO's opinion, the PNR do not, or do not clearly, bestow a function or power on the ISO, or provide a suitable process. The paper foreshadowed rule changes.

In response, some stakeholders contended that no or few rule changes were necessary, see rows 1 to 4 of this Appendix. In support of this contention, some advanced legal analyses asserting that some of the necessary functions or powers already exist in the rules. These are summarised briefly in the following rows.

Whatever these arguments' strengths or otherwise, the ISO does not propose to rely on them.

This review has identified several structural characteristics of the outage management process which merit change: it operates over too fast a timetable; it lacks formality, rigour and transparency; it lacks a mechanism for resolving disagreements and securing mitigations; and it is an opaque process open to only a subset of market participants. These features were a matter of deliberate design, hardwired into Subchapters 7.3 and 7.4 during the development of the 2021 regime. Changing these features should be done by explicit rule change, not by sometimes-strained inference.

Legal opinions can differ.¹⁴¹ The more subtle the legal reasoning needed to find the necessary power, the greater the risk of later disputes. Much better to make the position explicit, especially for matters as consequential as outage management and mitigation.

This review is not the end of the process. It is likely to result in rule change and procedure change proposals. When those proposals come forward, stakeholders will be welcome to argue that a particular change is unnecessary because the desired process, function or power already exists in the rules with adequate clarity and certainty.

48. That because the ISO's functions under rule 32(2)(b) and the Act include maintaining and improving system security, its functions already include all aspects of outage management.	The ISO proposes that this be made an explicit function, see Draft Recommendation 8.
49. Further that because the ISO's powers under rule 34 include whatever is necessary to perform the function in rule 32(2)(b), the ISO already has all the powers it needs to manage outages and to issue directions for that purpose.	The ISO proposes that these powers be made explicit, see Draft Recommendations 12, 15 and 16.
50. That the objectives set out in PNR rule 173(1) adequately prioritise the system security objective.	The ISO proposes that rule 173(1) be changed, so that it focusses directly on achieving the system security objective. See Draft Recommendation 7.
51. That the ISO already has adequate powers under Subchapters 7.3 and 7.4 to issue directions in respect of outage scheduling and mitigation.	The ISO proposes that these powers be made explicit, see Draft Recommendations 12, 15 and 16.
52. That the ISO could find the necessary power to issue directions by reading the definition of "scheduling conflict" in PNR rule 182(1) broadly, in effect to support ISO intervention whenever a proposed outage 'conflicts' with the system security objective, or similar.	The rules do not permit this reading, but in any event is rendered unnecessary by the proposed new process in section 7.3 and the new powers under Draft Recommendations 12, 15 and 16.
53. That PNR rule 53 gives the ISO adequate power to develop a new procedure.	The ISO proposes an explicit provision be added calling for an Outage Management Procedure, see Draft Recommendation 13.

¹⁴¹ For example, in feedback on the Issues Paper one stakeholder submitted that the ISO already has all the power it needs to issue directions about outage mitigation. But within the last 12 months, in the context of an actual outage, the same entity asserted exactly the opposite when rejecting an ISO request to do a thing to derisk the outage.

<p>54. That the ISO could use constraint rules to manage outages, and so no further powers were needed.</p>	<p>There will likely be a linkage between outage management and constraint rules, but they are two different processes. The ISO proposes the new process in section 7.3, with associated powers as per Draft Recommendations 12, 15 and 16. Perhaps, one of the resulting mitigations might be a constraint.</p>
<p>55. That existing ESS rules and arrangements provide an adequate means to deal with outage mitigation and recover the costs.</p>	<p>See row 44 of this Appendix and section 8.5.</p>
<p>56. That PNR rules 72(2) (ISO to identify planning criteria interactions) and 72(4)(b) (identify changes in ESS procurement), read with Chapter 8 and the <i>Harmonised Technical Rules</i>, provide an adequate mechanism to manage outage mitigation through ESS.</p>	<p>See rows 38 and 44 of this Appendix and section 8.5.</p>
<p>Other matters raised</p> <p><i>These matters are beyond the scope of this review. Stakeholders may wish to consider raising them with EPWA’s broader PNR Evolution review.</i></p>	
<p>57. A stakeholder raised the question of whether the ISO control desk should have full visibility across the NWIS, including Rio Tinto’s network.</p>	<p>—</p>
<p>58. A stakeholder queried whether rules participants could be confident that the system was getting the benefit of ESS for which the ISO had contracted (and NSPs were paying). This included comments on whether the current settings for required headroom level were correct.</p>	<p>—</p>
<p>59. A stakeholder expressed the view that the PNR do not deal adequately with the conflicts of interest inherent in vertically integrated NSPs having an operational role under the PNR and being members of Pilbara ISOCO Ltd.</p>	<p>—</p>
<p>60. Some stakeholders addressed Issue 5 from the Issues Paper (how outages affect system operating states) which the ISO has deferred to a broader review.</p> <p>One suggested that the determination of when the NWIS is in a “normal operating state” should be based on a risk assessment. Another suggested that a new operating state may be needed to deal with outages.</p>	<p>—</p>
<p>61. A stakeholder felt that the competition implications of the outage management regime should be regulated by the ACCC and not the PNR.</p>	<p>—</p>

Appendix 2: Relevant Rules

Subchapter 1.2 - Interpretation

...

8 Glossary

(1) A word or phrase defined below has the meaning given —

...

Contingency {also Contingency Event}: Means an event affecting the Power System involving the failure or removal from operational service of one or more Generating Units or Network Elements, or the disconnection at a Connection Point of a Registered Facility.

...

Pre-Contingent Threat: Means —

- a) a Credible imminent threat to the System Security Objective arising from —
 - i) an approaching external threat (such as a storm or bushfire); or
 - ii) impending material Equipment failure,
- or
- b) an imminent risk of physical injury or death to any person or material damage to Equipment,

which can be mitigated if appropriate preparatory measures (Pre-Contingent Actions) are taken.

...

Subchapter 7.1 – Key concepts

162 The System Security Objective

The “**System Security Objective**” is to —

- (a) Maintain the Power System Inside the Technical Envelope where practicable, and otherwise Promptly return it to Inside the Technical Envelope; and
- (b) Maintain the Power System in a Secure State where practicable, and otherwise return it to a Secure State as soon as practicable; and

- (c) otherwise — to a GEIP standard Maintain, and to a GEIP standard seek to improve, Security and Reliability.

163 Definition of Inside the Technical Envelope

- (1) The Power System is operating “**Inside the Technical Envelope**” whenever all of the following conditions are satisfied —
 - (a) the frequency at all energised busbars is within the Frequency Operating Standards set out in the Harmonised Technical Rules; and
 - (b) the voltage magnitudes are within the normal range set out in the Harmonised Technical Rules at all energised busbars in a switchyard or substation at a Generation Facility, or on a Transmission Network or Interconnector; and
 - (c) the MVA flows on all registered facilities and Network Elements are within the applicable Operating Ratings and Security Limits; and
 - (d) the Power System is configured such that the severity of any potential fault is within the capability of the relevant circuit breakers to disconnect the faulted circuit or Equipment.
- (2) The Power System is operating “**Outside the Technical Envelope**” whenever any of the conditions listed in rule 163(1) is not satisfied.

164 Definition of Secure State

The Power System is in a “**Secure State**” if it is —

- (a) operating Inside the Technical Envelope; and
- (b) subject to rule 72(4), expected to remain Inside the Technical Envelope following the occurrence of a single Credible Contingency event.

165 Definition of Normal Operating Conditions

A Power System is under “**Normal Operating Conditions**” when —

- (a) no Contingency has occurred; and
- (b) no Islands have formed; and
- (c) no System Operations Direction is in effect; and
- (d) frequency is within the Normal Frequency Tolerance Band; and
- (e) the Primary FCESS Provider is providing the Primary FCESS service in accordance with the Primary FCESS Contract; and
- (f) each contracted SRESS Provider is maintaining the amount of Headroom required by its SRESS Contract; and

- (g) electricity flows across Interconnectors are within the tolerances agreed by the Interconnected NSPs and notified to the ISO; and
- (h) no Pre-Contingent Actions are being taken.

166 Definition of Notifiable Event

A “**Notifiable Event**” for a Power System is any planned or anticipated system event (including a planned Outage, commissioning or testing of a Facility or Network Element) which might credibly be expected to adversely affect —

- (a) Security or Reliability; or
- (b) the ability of any part of a Covered Transmission Network to benefit from Essential System Services; or
- (c) the ability of a Covered NSP to provide Transmission Voltage contracted Network services.

167 Definition of System Coordination Matters

The following are “**System Coordination Matters**” —

- (a) the scheduling and coordination of all planned or anticipated Notifiable Events; and
- (b) any changed circumstances or material new information regarding any planned or anticipated Notifiable Event; and
- (c) for each currently planned or anticipated Notifiable Event —
 - (i) its likely consequences for Security and Reliability; and
 - (ii) its likely consequences in terms of whether a Constraint Rule is, or is likely, to be violated; and
 - (iii) any measures, which may be necessary or desirable to put in place for managing the Power System in order to achieve the System Security Objective during the event, including any changes in Essential System Service procurement, configuration, Enablement or Dispatch; and
 - (iv) if it is a planned Outage — whether the Outage should proceed as planned or at all;and
- (d) any other matters affecting Security, Reliability or system operations generally which are appropriate for discussion under Subchapter 7.3.

Subchapter 7.3 – System coordination

173 Objectives of this Subchapter 7.3 and Subchapter 7.4

- (1) The primary objective of this Subchapter 7.3 and Subchapter 7.4 is to —
 - (a) promote communication and collaboration between the ISO and Registered NSPs regarding System Coordination Matters; and
 - (b) in so doing provide the ISO, Registered NSPs and ESS Providers with the information they reasonably need to perform their obligations under these Rules and relevant contracts, with a view to achieving the System Security Objective; and
 - (c) promote the collaborative resolution of Scheduling Conflicts regarding Outages and other System Coordination Matters; and
- (2) The secondary objectives of this Subchapter 7.3 and Subchapter 7.4 is to do the above things in as efficient and informal a manner as practicable, maximising communication while minimising the compliance burden.

174 System coordination meetings

- (1) The ISO is to convene a system coordination meeting at least once every fortnight.
- (2) The system coordination meeting is to discuss, as necessary, any or all current and anticipated System Coordination Matters.
- (3) A system coordination meeting is to be attended by —
 - (a) from each Registered NSP, a manager who has Direct operational responsibility for the personnel of an NSP who are engaged in system operations activities, or the manager's alternate; and
 - (b) an ISO representative, who is to chair the meeting.
- (4) Unless the chair determines otherwise after consulting the Registered NSP representatives —
 - (a) the system coordination meeting's duration should normally not exceed 30 minutes; and
 - (b) a person identified in rule 174(3) may appoint an alternate from time to time; and
 - (c) the chair may permit one further ISO or Registered NSP representative to attend the meeting, to provide secretarial support; and
 - (d) otherwise, no-one else may attend a system coordination meeting.

{The intention is that meetings will predominantly involve the 4 people identified, and no-one else. The chair may from time to time invite others to attend, for example representatives from an ESS Provider or a major Load, but this is not intended to be a regular occurrence.}

- (5) The ISO and Registered NSPs may agree on arrangements for system coordination meetings which differ from this rule 174.

175 Activities between system coordination meetings

Between system coordination meetings, the ISO will liaise as necessary with Registered NSPs and ESS Providers regarding System Coordination Matters.

176 System coordination meetings and discussions – Confidential Information

- (1) A person who participates in a meeting or discussion under this Subchapter 7.3 or Subchapter 7.4 must —
 - (a) ensure that any Confidential Information it obtains in the course of the meeting or discussion is not disclosed or accessible beyond the person's operational staff (except to the extent reasonably necessary for audit, compliance and governance purposes); and
 - (b) not use, store, analyse or disseminate any Confidential Information it obtains in the course of the meeting or discussion, for any purpose other than the purposes of this Subchapter 7.3 or Subchapter 7.4 or otherwise seeking to achieve the System Security Objective.
- (2) Rule 176(1) does not limit Subchapter 11.2 { Confidential Information}.

177 ISO to produce System Coordination Report

- (1) After each system coordination meeting, and otherwise as it considers necessary, the ISO must give to the Registered NSPs and ESS Providers a report on —
 - (a) any current or anticipated System Coordination Matters; and
 - (b) any follow-up actions the ISO considers appropriate, including further discussions and the provision of further information; and
 - (c) any other thing the ISO recommends be done or not done, in respect of any of those matters.
- (2) The format and content of the System Coordination Report is to be determined by the ISO from time to time in consultation with the Registered NSPs, placing an emphasis on meeting the objectives in rule 173 as simply and efficiently as practicable.
- (3) The System Coordination Report is to be based upon information received by the ISO —
 - (a) at system coordination meetings;
 - (b) from Registered NSPs' internal Outage planning reports provided under rule 180(2)(b);
 - (c) otherwise from Registered NSPs.

- (4) The ISO may inform itself as it sees fit in Connection with this Subchapter 7.3 and Subchapter 7.4, but does not have a general obligation to investigate planned or anticipated Notifiable Events beyond the information sources set out in rule 177(3).

178 Review of this Subchapter 7.3 and Subchapter 7.4

- (1) From time to time, and at least once in every five year period starting from the Rules Commencement Date, the ISO must conduct a review of the processes set out in this Subchapter 7.3 and Subchapter 7.4 against the Pilbara Electricity Objective.
- (2) The review must include consultation with Registered NSPs and registered controllers and Public consultation following the Expedited Consultation Process.
- (3) At the conclusion of a review, the ISO must Publish a report containing any recommended changes to this Subchapter 7.3 or Subchapter 7.4.
- (4) If the ISO recommends any Rules or Procedure changes in the report, it must either submit a Rule Change Proposal or initiate a Procedure Change Process, as the case may be.

Subchapter 7.4 – Notifying planned and unplanned Outages

179 If a near-term event arises between system coordination meetings

- (1) If a Registered NSP, the ISO or the ISO Control Desk becomes aware of a pending Notifiable Event which has not previously been notified and is likely to occur before the next system coordination meeting, then (without limiting rule 183) it must take reasonable steps to a GEIP standard Promptly to notify, and coordinate with, as the case may be, the other Registered NSPs and the ISO Control Desk regarding the Notifiable Event.
- (2) Rule 179(1) applies also to a previously-notified Notifiable Event if there is a material change from the circumstances as previously notified.

180 Notification obligations

- (1) Each Registered NSP must notify the ISO and the other Registered NSPs of each planned or anticipated Notifiable Event on its Network, and must (to an extent which is reasonable having regard to the objectives in rule 173) keep them updated as information about the Notifiable Event changes.
- (2) Subject to rule 179, a Registered NSP will be deemed to have complied with its obligation under rule 180(1) if it —

- (a) provides the information orally at the next system coordination meeting;

{There is no minimum advance warning period for planned Outages. However, the effect of rule 180(2)(a) is to oblige the Registered NSP to raise a planned Outage at the system coordination meeting as soon as it appears on the Registered NSP's own planning horizon.}

and

- (b) Promptly gives the ISO a copy of the Registered NSP's internal Outage planning report each time the internal report is materially updated.
- (3) A Registered NSP may redact commercially sensitive information from a report given to the ISO under rule 180(2)(b).

181 Outages of facilities

- (1) Each Registered NSP must ensure that it is kept sufficiently informed about Notifiable Events affecting facilities Connected to its Network, to Enable it to comply with its obligations under Subchapter 7.3 and this Subchapter 7.4.
- (2) If a Registered Facility is Connected to a Covered Network, then the Registered Controller must keep the Covered NSP sufficiently informed about Notifiable Events affecting the Registered Facility, to Enable Registered NSPs and the ISO to comply with their obligations under Subchapter 7.3 and this Subchapter 7.4.

182 Resolving Scheduling Conflicts

- (1) A “**Scheduling Conflict**” arises for a planned Outage if the ISO determines that the Outage taken together with all currently proposed or anticipated Notifiable Events, may cause the Power System to be Outside the Technical Envelope, or otherwise poses an unacceptable risk to Security and Reliability.
- (2) Wherever possible, Scheduling Conflicts are to be resolved by consensus between the Registered NSPs, facilitated as necessary by the ISO.
- (3) If the ISO determines that a consensus will not be reached in time for the relevant Notifiable Events to be managed appropriately, the ISO may resolve the Scheduling Conflict by giving a Direction to one or more of the affected parties but cannot give such a direction to the Pluto Facility's Controller.
- (4) If the Scheduling Conflict involves, or involved facilities in, both a Covered Network and an integrated Mining System, the ISO must have regard to rule 5 in determining the content of a Direction under rule 182(3).
- (5) A Direction under rule 182(3) may specify which Notifiable Event is to have priority for scheduling purposes, and may contain such scheduling or other information or instructions as the ISO considers reasonably necessary to resolve the Scheduling Conflict and achieve the System Security Objective.

183 Obligations to report contingencies and unplanned events

- (1) The Registered NSP in whose Network a Notifiable Unplanned Event {defined in rule 183(5)} occurs, must Promptly on a 24/7 Basis notify the other Registered NSPs and the ISO Control Desk.
- (2) An ESS Provider who suffers an unplanned Outage which will impact its ability to provide Essential System Services, must Promptly on a 24/7 Basis notify all Registered NSPs and the ISO Control Desk.

- (3) A Generator who suffers an unplanned Outage of any Generating Unit which will or might credibly be a Notifiable Unplanned Event, must Promptly on a 24/7 Basis notify all Registered NSPs and the ISO Control Desk.
- (4) The Protocol Framework is to set out communication requirements for notifications under this rule 183.
- (5) In rule 183(1), an “**Notifiable Unplanned Event**” for a Network means any Contingency or other event, that might impact the Network in a way which might credibly be expected to adversely affect —
 - (a) achievement of the System Security Objective; or
 - (b) any part of a Covered Transmission Network’s ability to benefit from Essential System Services; or
 - (c) a Covered NSP’s ability to provide Transmission Voltage contracted Network services.

Appendix 3: WEM Outage Process

The following is an extract from AEMO *Wholesale Electricity Market Design Summary*, September 2023 (available [here](#)), section 6.5.

“6.5 Outages⁶⁴”

Good visibility of future Network and Facility Outages is essential to assist participants in effective availability planning for their Facilities, and for producing overall efficient market outcomes. Network Outages, in particular, can have a pronounced impact on the levels of network congestion, which flows on to the ability to schedule and dispatch sufficient generation to meet demand.

⁶⁴ The Outage planning processes are covered in detail in clauses 3.18 to 3.20 of the WEM Rules

Market Participants are required to tell AEMO when their Registered Facilities are unavailable for dispatch by submitting Planned Outages and Forced Outages through AEMO’s systems. Participants must have approval for Planned Outages and must provide information about Forced Outages as soon as possible. There are two main reasons for this:

- AEMO needs this information to accurately forecast expected power system conditions, including reserve margins and appropriate Constraints Sets for use in the Dispatch Algorithm. They can reject an Outage request if necessary to ensure sufficient capacity will be available to meet projected demand for energy and ESS and to ensure PSR and PSS can be maintained.
- Participants receiving capacity payments through the RCM are compensated for making their Facilities available. If a Facility is not available because of an unplanned or unapproved Outage, it is not meeting its Reserve Capacity Obligations, and thus, part of the capacity payment must be paid back. The details of the Outage are used to calculate the size of the capacity refund.

6.5.1 Participation in the Outage process

AEMO compiles a list of all equipment on the power system that is required to schedule Outages, including partial Outages and de-ratings⁶⁵. This list includes Facilities holding Capacity Credits⁶⁶, Facilities that provide ESS, items of network equipment that could limit the output of such Facilities, and any other equipment that could affect the PSS and PSR. Market Participants may request that AEMO reassess the inclusion of their equipment on this list.

Facilities not on the Equipment List are known as Self Scheduling Outage Facilities (SSOFs). Participants must still submit Outage Plans for SSOFs, but the Outage Plans are not subject to AEMO assessment, and are deemed approved unless explicitly rejected by AEMO for not meeting required submission deadlines or misrepresenting availability status.

6.5.2 Outage approval

Market Participants can request approval for Planned Outages with specific start and end Dispatch Intervals up to three years ahead. The request must include:

- The reason for, timing of, and duration of the proposed Outage.
- Potential risks to the intended duration of the Outage.
- Contingency plans should the Facility need to be returned to service prior to the scheduled Outage Completion time. Except in a few limited situations (such as when requesting an extension of a Planned Outage currently underway), a request for a Planned Outage can only be made where the participant reasonably believes that the Facility would otherwise be available for service.

Planned Outage requests must indicate the Remaining Available Capacity (RAC) for dispatch during the Outage. For a full Outage (where the Facility is completely unavailable), the RAC would be 0 MW. For partial and overlapping Outages, the RAC can vary over the duration of the Outage. Where a Planned Outage impacts the provision of an ESS or relates to a component of the Facility that has been separately accredited for Reserve Capacity, the Outage request must also include information on each affected service and component.

⁶⁵ At <https://aemo.com.au/-/media/files/electricity/wem/data/system-management-reports/equipment-list.pdf>.

⁶⁶ Excluding Demand Side Programmes.

While participants can request Outages up until two days before the event — or even up to two hours ahead for ‘Opportunistic Maintenance’ Outages of less than 24 hours — AEMO may reject a request if there is insufficient time to assess the impact of the Outage. Most Outages are notified to AEMO well in advance of their commencement, and in many cases more than a year before the event.

AEMO will usually review Outage Plans in the order received, and will approve an Outage Plan provided sufficient energy supply and network capacity will remain to maintain PSR and PSS. Once approved, Outage Plans continue to be reviewed periodically by AEMO to ensure they can still be accommodated as power system conditions change (for example, where Unplanned Outages occur). When changed conditions may result in an Outage potentially needing to be re-scheduled, AEMO will notify the Market Participant that the Outage is ‘at risk’. Approved Outages are also subject to a final check with the AEMO control room before commencing, with certain equipment requiring ‘permission to proceed’ to ensure the supporting configuration is in place (such as applying appropriate Constraints in the Dispatch Algorithm). Permission to proceed would typically only be denied if something unusual or unexpected is occurring.

Rule Participants must advise AEMO of changes to previously submitted Outage Plans, and must formally withdraw an Outage Plan if they are no longer planning to make the equipment unavailable.

AEMO publishes information on submitted Outage Plans on the WEM Website, including status, timing, and details of the affected equipment or services.

6.5.3 Forced Outages

Participants must also advise AEMO of Forced (unplanned) Outages:

- Participants must notify the AEMO control room as soon as possible with initial information on the Forced Outage, such as the affected equipment or service, the Remaining Available Capacity, the nature of the failure, and any indicative restoration timeframe.
- Participants must submit a Forced Outage entry with full details of the Outage into AEMO's Outage system no later than the end of the next Business Day after the day the Forced Outage occurred.
- Participants must update the Forced Outage entry with any material changes to Forced Outage information as soon as practicable, with final information required no later than 15 calendar days after the day the Forced Outage occurred.
- If AEMO becomes aware of New Information relating to a Forced Outage, it can require a participant to submit or revise a Forced Outage entry, even after 15 calendar days.

Forced Outage data is used to calculate any required Reserve Capacity refunds. AEMO publishes Forced Outage information on the WEM Website.

6.5.4 Outage Intention Plans

By 1 March every year, Market Participants and Network Operators must submit a non-binding 'Outage Intention Plan' listing their intentions for Outages in the next calendar year, providing indicative information for expected Outages which have not yet been submitted⁶⁷. This information helps coordinate network and Facility Outages. AEMO uses the information provided to construct and publish a consolidated Outage Intention Plan covering all

⁶⁷ Self-Scheduling Outage Facilities are exempt from this requirement. Self-Scheduling Facilities are small Facilities such as Non-Scheduled Facilities whose Outages AEMO does not require visibility of.

Rule Participants. Where individual participant plans conflict, AEMO and participants work together to find an alternative plan. While Outage Intention Plans are not binding on participants or AEMO and individual Outages must still be requested and approved via the normal process, Outages signalled in an Outage Intention Plan do have some priority over Outages not included in an Outage Intention Plan.

6.5.5 Outage coordination

Some network Outages affect the ability of Market Participants to operate their Facilities as they wish. For example, a line Outage could mean that maximum Injection from a Facility cannot be accommodated by the remaining network components. It is generally desirable, but not always possible, to schedule these network Outages at mutually agreeable times. Network Operators are required to notify Impacted Participants and seek mutual agreement on Outage timing, before submitting the Outage Plan to AEMO at least six months in advance. If no agreement is reached, the Impacted Participant may request that AEMO determine whether the proposed Outage Plan should be revised, having regard to:

- Maintaining PSR and PSS.

- The relative dates on which the Outage was notified.
- Whether the Outages were signalled in an Outage Intention Plan.
- The urgency of any required maintenance, and the impacts of not performing that maintenance.
- The impacts of rescheduling the Outage.

Where AEMO rejects an Outage Plan, the affected participant can appeal to the ERA, but only on the grounds that AEMO has not met the requirements of the WEM Rules or the relevant WEM Procedure.

6.5.6 Outage cancellation and recall

Sometimes AEMO needs to recall or cancel an Outage it has previously approved. If power system conditions or forecasts change after an Outage is approved, AEMO can notify a participant that its Outage is 'at risk' of rejection. If proceeding with the Outage poses a risk to PSS or reliability, AEMO may reject the Outage or recall the Facility to service early. When rescheduling, Outages that were previously rejected or recalled in this way get priority over new Outages.

If an Outage is submitted at least a year prior to commencement, then approved, and then rejected within

48 hours of its commencement or recalled by AEMO, the affected party can apply for Outage Compensation to cover additional maintenance costs directly incurred in relation to the rejection or recall. Compensation is funded from Market Participants based on their energy consumption in the affected Trading Intervals.

6.5.7 Effect of Outages on Reserve Capacity Obligations

When Planned Outage requests are approved by AEMO, they are designated as Planned Outages, and the Reserve Capacity Obligation Quantity (RCOQ) of the affected Facility is reduced to reflect the Outage during the impacted Trading Intervals. If the Facility has Planned Outages with duration totalling more than approximately six months over a rolling 1,000-day horizon, the RCOQ is not reduced, and the Market Participant will be required to refund Reserve Capacity Payments.

All other Outages are Forced Outages. As described in Section 6.5.3, Market Participants are obliged to inform AEMO of Forced Outages as soon as practicable, and to provide information concerning when the Facility will

return to service. Market Participants are required to refund Reserve Capacity payments when their Facilities suffer Forced Outages (see Section 7.4.3). For the purposes of refund calculations, Charge Level shortfalls for Electric Storage Resources are treated as Forced Outages.”