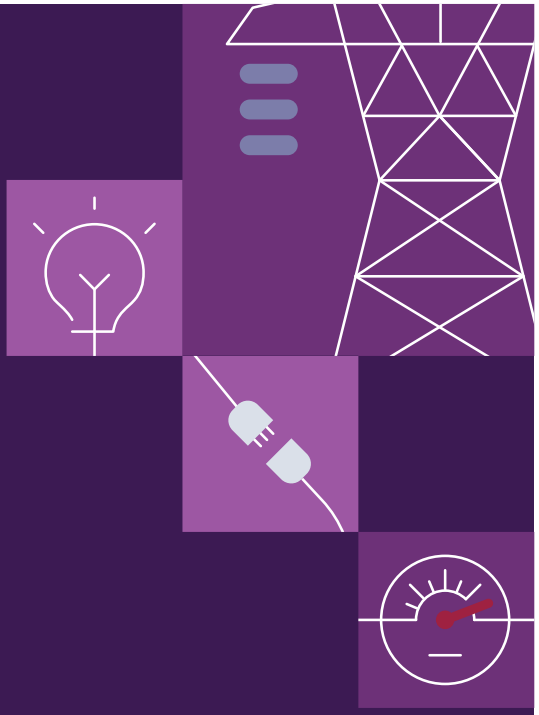
AEMO
AUSTRALIAN ENERGY MARKET OPERATOR



Security Enablement Procedures

Consultation paper - Standard consultation for the National Electricity Market

Published: 07 April 2025

aemo.com.au

New South Wales | Queensland | South Australia | Victoria | Australian Capital Territory | Tasmania | Western Australia

Australian Energy Market Operator Ltd ABN 94 072 010 327

Explanatory statement and consultation notice

This consultation paper commences the first stage of the standard rules consultation procedure conducted by AEMO to consider proposed content for the Security Enablement Procedures (**proposal**) under National Electricity Rules (**NER**) 4.4A.6(a). The standard rules consultation procedure is described in NER 8.9.2.

Context

On 28 March 2024, the Australian Energy Market Commission (AEMC) made a final determination in relation to the *Improving security frameworks for the energy transition* rule change[1]. The determination introduced the National Electricity Amendment (Improving security frameworks for the energy transition) Rule 2024 (ISF Rule)[2] to improve market arrangements for security services. The ISF Rule evolves existing frameworks with the aim of ensuring sufficient security services are provided as the power system continues to transition to higher penetrations of inverter-based resources (IBR). It requires AEMO to assess and enable the necessary security services in operational timeframes to ensure that the power system is secure day-to-day[3].

The enablement of all security services under the ISF Rule commences 2 December 2025 and must be conducted in accordance with the Security Enablement Procedures that are to be published by 31 August 2025. On 30 June 2024, AEMO published Provisional Security Enablement Procedures (Provisional Procedures) under NER 11.168.2(b) that set out the minimum or recommended requirements to be included in agreements for the provision of system security services entered into by transmission network service providers (TNSPs).

The Security Enablement Procedures build on the Provisional Procedures and, in addition to requirements in agreements to be entered by TNSPs, include:

- a methodology for how AEMO will determine the minimum system security requirements
- a methodology for how AEMO will enable the system security requirements in accordance with the principles set out in clause 4.4A.4, and
- how AEMO determines, and enables system strength services to support, the level of stable voltage waveform requirements.

In developing these procedures, AEMO has focused on developing a framework that allows enablement of security services in a transparent fashion and evolution over time. This includes:

- the application of limits advice through constraints in the same way as other power system limits
- the assessment of security service needs over the pre-dispatch timeframe and any impact of enablement on pre-dispatch outcomes.

A draft version of the Security Enablement Procedures has been provided as part of this consultation process. AEMO acknowledges that some sections may change as issues are worked through with stakeholders via this consultation and to accommodate timing considerations around AEMO's progressive implementation approach.

This consultation will also cover consequential amendments to the:

[1] https://www.aemc.gov.au/sites/default/files/2024-03/ERC0290%20-%20ISF%20final%20determination.pdf

[2] https://www.aemc.gov.au/sites/default/files/2024-04/Final%20Rule%20-%20in%20mark%20up.pdf

[3] https://www.aemc.gov.au/sites/default/files/2024-03/ERC0290%20-%20ISF%20final%20determination.pdf, page i

- SO_OP_3708 Non-market Ancillary Services (including the Guide to Ancillary Services in the NEM)
- SO_OP_3704 Pre-Dispatch Procedure
- Spot market operations timetable
- SO_OP_3718 Outage Assessment, and
- SO_OP_3715 Power System Security Guidelines.

Consequential amendments to the Constraint Formulation Guidelines (CFG) and the Schedule of Constraint Violation Penalty Factors (SCVPF) will be managed separately, and not form part of this consultation, as required changes cannot be determined in the same timeframe.

AEMO intends to provide marked versions of these documents at the draft report stage of this consultation.

Proposal

AEMO proposes content for the Security Enablement Procedures, considering:

- alignment with the NSCAS Descriptions and Quantities Procedure
- alignment with the System Strength Requirements Methodology
- alignment with the Inertia Requirements Methodology, and
- TNSP limits advice on the stable voltage waveform requirements for efficient levels of system strength.
- AEMO's development timelines and an incremental approach to expanding automated enablement process capability from December 2025

For detailed information on the proposal and AEMO's reasoning, please refer to the subsequent sections of this consultation paper.

Consultation notice

AEMO is now consulting on this proposal and invites written submissions from interested persons on the issues identified in this paper to **NEMReform@aemo.com.au** by 5:00 pm (Melbourne time) on 08 May 2025.

Submissions may make alternative or additional proposals you consider may better meet the objectives of this consultation and the national electricity objective in section 7 of the National Electricity Law. Please include supporting reasons.

Before making a submission, please read and take note of AEMO's consultation submission guidelines, which can be found at https://aemo.com.au/consultations. Subject to those guidelines, submissions will be published on AEMO's website.

Please identify any parts of your submission that you wish to remain confidential, and explain why. AEMO may still publish that information if it does not consider it to be confidential, but will consult with you before doing so. Material identified as confidential may be given less weight in the decision-making process than material that is published.

Submissions received after the closing date and time will not be valid, and AEMO is not obliged to consider them. Any late submissions should explain the reason for lateness and the detriment to you if AEMO does not consider your submission.

Interested persons can request a meeting with AEMO to discuss any particularly complex, sensitive or confidential matters relating to the proposal. Please refer to NER 8.9.1(k). Meeting requests must be received by the end of the submission period and include reasons for the request. AEMO will try to accommodate reasonable meeting requests but, where appropriate, we may hold joint meetings with other stakeholders or convene a meeting with a broader industry group. Subject to confidentiality restrictions, AEMO will publish a summary of matters discussed at stakeholder meetings.

Contents

Tables

Figures

1. Stakeholder consultation process

As required by the National Electricity Rules (NER) clause 4.4A.6, AEMO is consulting on the Security Enablement Procedures (proposal) in accordance with the standard rules consultation procedure in NER 8.9.2. AEMO has also conducted a series of meetings and one-on-one engagements with TNSPs in 2024 and early 2025 to inform the preparation of this consultation paper and the Security Enablement Procedures.

NER 11.168.2 requires AEMO to publish the first Security Enablement Procedures by 31 August 2025. The proposal also covers consequential changes to the following documents, which are required as a result of the ISF Rule:

- SO_OP_3708 Non-market Ancillary Services
- SO_OP_3704 Pre-Dispatch Procedure
- Spot market operations timetable
- SO_OP_3718 Outage Assessment, and
- SO_OP_3715 Power System Security Guidelines.

The proposal does not include consequential changes to:

- Schedule of constraint violation penalty factors (SCVPF), or
- Constraint Formulation Guidelines (CFG).

These documents will be consulted on at a later time.

Note that this document uses terms defined in the NER, which are intended to have the same meanings. There is a glossary of additional terms and abbreviations in Appendix A.

AEMO's indicative process and timeline for this consultation are outlined below. Future dates may be adjusted and additional steps may be included if necessary, as the consultation progresses.

Consultation steps	Dates
Publication of Provisional Security Enablement Procedures	30 June 2024
Consultation paper published	7 April 2025
Briefing to Electriciy Wholesale Consultative Forum	8 April 2025
Stakeholder forum	10 April 2025
Submissions due on consultation paper	8 May 2025
Draft report published	Expected 6 June 2025
Submissions due on draft report	Expected 8 July 2025
Final report and procedure published	Expected 4 August 2025

1.1. Register for the upcoming public forum

AEMO has scheduled a public forum to discuss the issues raised in this consultation paper, on

10 April 2025, from 1:00-2:30pm AEST. Please click here to register for that event.

AEMO and consultation stakeholders may continue to request meetings or further information when required.

Questions

1. What specific areas would you like more in depth briefings from AEMO on?

2. Background

2.1. Context for this consultation

Under the National Electricity Amendment (Improving security frameworks for the energy transition) Rule 2024 (ISF Rule)[4], AEMO has been given a new power to enable system security services provided or procured by TNSPs or procured by AEMO to meet minimum system security requirements and to meet stable voltage waveform requirements.

The intention of this framework is to enable the most cost efficient system security services available to maintain system security in the transition to a low- or zero-emissions power system, and system strength services to meet stable voltage waveform requirements when appropriate to do so.

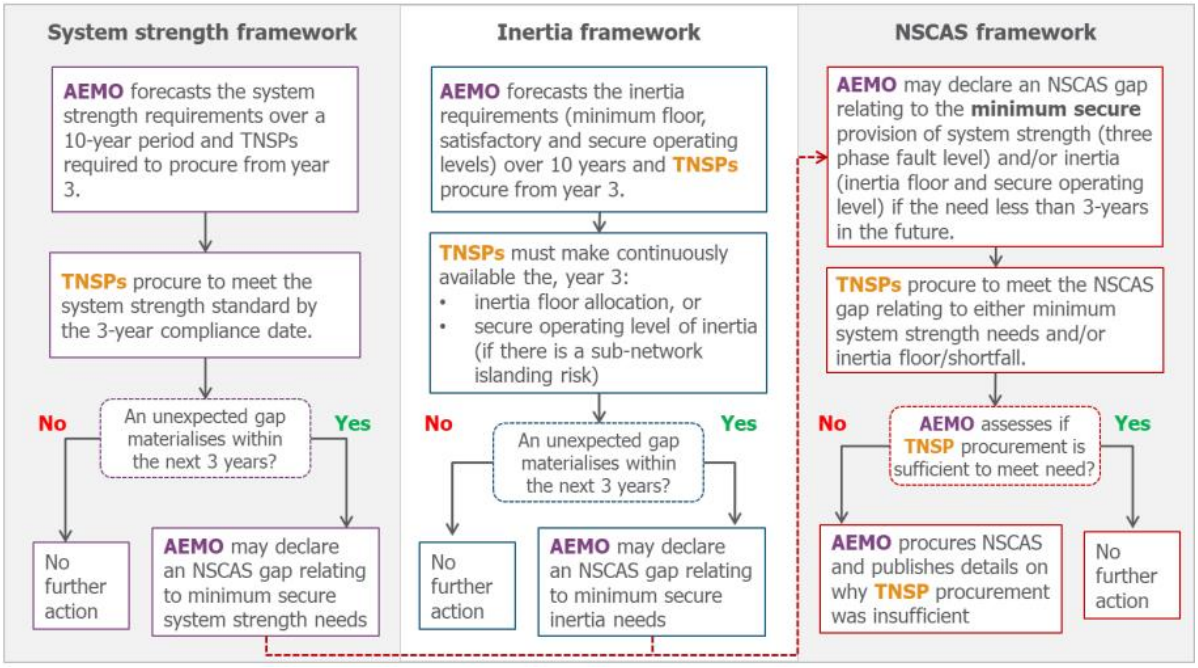
System security services include system strength services, inertia network services, network support and control ancillary services (NSCAS), and transitional services (introduced by ISF Rule). Figure 1 illustrates the interaction between frameworks that are the subject of the Security Enablement Procedures. Transitional services, introduced under the ISF Rule, are also the subject of these procedures but are not included in Figure 1 as they do not relate to system strength or inertia. The same applies to NSCAS that is not related to system strength or inertia, for example, voltage control.

AEMO is taking an incremental approach to the implementation of the new system security services enablement framework under the ISF Rule. The intention is to agree an approach in consultation with industry that is achievable in the timeframes allowed, ensures compliance with the regulatory framework and provides an ongoing opportunity to develop the framework further as understanding of the available services, their enablement capabilities, the ongoing need and the impact of enablement on electricity market operation deepens.

The Security Enablement Procedures establish how AEMO will determine the minimum system security and stable voltage waveform requirements and the methodology by which system security services will be enabled to meet these requirements.

[4] https://www.aemc.gov.au/rule-changes/improving-security-frameworks-energy-transition

Figure 1 Interaction between system strength, inertia and NSCAS frameworks[5]



Note: From Australian Energy Market Commission (**AEMC**) Final Determination, page 37 Figure 3.8

2.2. NER requirements

NER 11.168.2 provides that AEMO must publish the first Security Enablement Procedures by 31 August 2025.

NER 4.4A.6 specifies the following requirements for the Security Enablement Procedures that are the subject of this consultation paper:

(a) AEMO must develop and publish procedures for the enablement of system security services (Security Enablement Procedures), which must include:

(1) a methodology for how AEMO will determine the minimum system security requirements in accordance with clause 4.4A.3;

(2) a methodology for the enablement of system security services in accordance with the enablement principles in clause 4.4A.4;

(3) any minimum or recommended requirements to be included in agreements for the provision of system security services entered into by Transmission Network Service Providers; and

(4) a description of how AEMO determines the level of stable voltage waveform requirements under clause 4.4A.1(b) and how it will enable system strength services under a system strength services agreement to support this level.

(b) AEMO must comply with the Rules consultation procedures when making or amending the Security Enablement Procedures.

[5] While this figure shows the relationship between these three frameworks, the scope of NSCAS gap declarations is broader than only System Strength and Inertia. NSCAS can include any characteristic necessary to maintain the security and supply reliability of the transmission network in accordance with the power system security standards and the reliability standard.

2.2.1. Enablement of system security services.

NER 4.4A.1 establishes the objective of system security service enablement that informs the Security Enablement Procedures:

> *AEMO may, at any time, enable:*
>
> *(a) any system security services to achieve and maintain the minimum system security requirements; and*
>
> *(b) system strength services to achieve and maintain stable voltage waveforms for the level and type of inverter based resources and market network service facilities that AEMO forecasts would be dispatched in the relevant trading interval if this were not limited by system strength services (stable voltage waveform requirements),*
>
> *in accordance with this rule 4.4A and the Security Enablement Procedures.*

2.2.2. System security services

NER 4.4A.6 references *system security services*. These are defined in NER 4.4A.2 as each of the following:

> *(a) a system strength service;*
>
> *(b) an inertia network service;*
>
> *(c) a NSCAS; and*
>
> *(d) a transitional service,*
>
> *to the extent procured by AEMO or a Transmission Network Service Provider under an agreement for that service under the Rules.*

2.2.3. Minimum system security requirements

NER 4.4A.6(a)(1) references *minimum security requirements*. These are defined in NER 4.4A.3 which requires AEMO to publish the *minimum system security requirements* from time to time in accordance with the Security Enablement Procedures:

> *(b) The minimum system security requirements are those necessary for the operation of the power system during the range of actual operating conditions encountered in the power system including:*
>
> *(1) the inertia sub-network allocation for each inertia sub-network;*
>
> *(2) where a contingency event that would result in an inertia sub-network becoming islanded has been classified as a credible contingency event or defined as a protected event, the level of inertia reasonably considered necessary by AEMO to operate the inertia sub-network so that it is and will remain in a satisfactory operating state when the inertia sub-network is islanded;*
>
> *(3) where an inertia sub-network is islanded, the level of inertia reasonably considered necessary by AEMO to operate the inertia sub-network so that it is and will remain in a secure operating state;*
>
> *(4) the minimum three phase fault level for each system strength node reasonably considered necessary by AEMO to maintain the power system in a secure operating state;*
>
> *(5) a NSCAS need to the extent reasonably considered necessary by AEMO to maintain the power system in a secure operating state;*
>
> *(6) the power system security needs and expected duration specified in the statement for transitional services published under clause 3.11.12(a)(2)(i) from time to time, where applicable; and*

(7) *any other power system security requirements that AEMO determines from time to time are necessary to maintain the power system security standards, but does not include the reliability standard or the system restart standard.*

(c) *The minimum system security requirements:*

(1) *are not required to be consistent with the binding inertia requirements and binding system strength requirements;*

(2) *may exceed those requirements where reasonably necessary for AEMO to achieve the minimum system security requirements; and*

(3) *where they are different to those requirements, do not affect the relevant Inertia Service Provider's or System Strength Service Provider's obligation to make inertia network services or system strength services available in accordance with the binding inertia requirements and binding system strength requirements.*

2.2.4. System security service enablement principles

NER 4.4A.6(a)(2) references enablement principles. These are defined in NER 4.4A.4 and AEMO is required to use reasonable endeavours to give effect to these principles when enabling services under 4.4A.1:

(a) *the system security services that are enabled should be the lowest total cost combination required to achieve and maintain the minimum system security requirements and the stable voltage waveform requirements;*

(b) *a system security service should be enabled as close as practicable to the relevant trading interval, and in any case, enabled no more than 12 hours ahead of the trading interval;*

(c) *a system security service should only be enabled where, in AEMO's reasonable opinion, the minimum system security requirements or the stable voltage waveform requirements would not be met but for such enablement;*

(d) *when enabling a system security service to achieve the stable voltage waveform requirements, where such services are required in addition to those required to achieve the minimum system security requirements, AEMO should:*

(1) *only enable a quantity of system strength services that is reasonably necessary to achieve stable voltage waveforms for the level and type of inverter based resources and market network service facilities that AEMO projects could be dispatched in the relevant trading interval; and*

(2) *not enable a system strength production unit if enabling that unit would result in significant adverse effects on power system efficiency or power system emissions.*

2.2.5. Instructions to enable system security services

NER 4.4A.5 provides AEMO with the ability to instruct a provider of system security services (**Provider**) to enable or cease enablement of a service in accordance with the enablement principles. It requires the Provider to ensure that it can receive and respond to an instruction in accordance with the relevant procedures and if required make adjustment to dispatch bids under NER 3.8.22.

2.3. The national electricity objective

Within the specific requirements of the NER applicable to this proposal, AEMO will seek to make a determination that is consistent with the national electricity objective (**NEO**) and, where considering options, to select the one best aligned with the NEO.

The NEO is expressed in section 7 of the National Electricity Law as:

> *to promote efficient investment in, and efficient operation and use of, electricity services for the long term interests of consumers of electricity with respect to:*
>
> *(a) price, quality, safety, reliability and security of supply of electricity; and*
>
> *(b) the reliability, safety and security of the national electricity system; and*
>
> *(c) the achievement of targets set by a participating jurisdiction—*
>
> *(i) for reducing Australia's greenhouse gas emissions; or*
>
> *(ii) that are likely to contribute to reducing Australia's greenhouse gas emissions.*

3. Security Enablement Procedures

The Security Enablement Procedures are required to address four key areas. At a high level, these are:

1. minimum system security requirements methodology
2. enablement methodology in accordance with the enablement principles
3. requirements in TNSP system security agreements, and
4. how AEMO determines and enables stable voltage waveform requirements.

These areas are discussed in the following sections.

3.1. Minimum system security requirements methodology

The Procedures describe how AEMO will enable system security services to meet minimum system security requirements in the operational timeframe[6]. The Procedures also include the methodology that AEMO will use in determining those requirements.

The minimum system security requirements are those necessary for AEMO to operate the power system in a *secure operating state*[7] and to allow AEMO to meet the *general principles for maintaining power system security*[8] during the range of actual operating conditions encountered in the power system. The key requirement is that AEMO should operate the power system in a secure operating state and at all times be able to return the power system to secure operating state within 30 minutes of a contingency event.

Where minimum system requirements are not expected to be met (that is, there is a gap), AEMO will enable available services to fill that gap in accordance with the security enablement methodology. AEMO publishes the following documents that describe the methodologies for establishing system strength, inertia and other system security (NSCAS and transitional services) needs in the planning timeframe.

- the Inertia Requirements Methodology made under NER 5.20.4[9], and the associated annual Inertia Report[10]
- the System Strength Requirements Methodology made under NER 5.20.6[11], and the associated annual System Strength Report[12]

[6] These will typically be derived consistent with the security *investment* requirements that apply in the planning timeframe, but with consideration given to the more nuanced, dymamic, or extreme system conditions observed operationally.

[7] A *Secure Operating State* as defined by NER clause 4.2.4.

[8] The *General principles for maintain power system security* as outlined in NER clause 4.2.6.

[9] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/inertia-requirements-methodology-v2-0.pdf

[10] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/2024-inertia-report.pdf

[11] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system-strength-requirements/system-strength-requirements-methodology.pdf

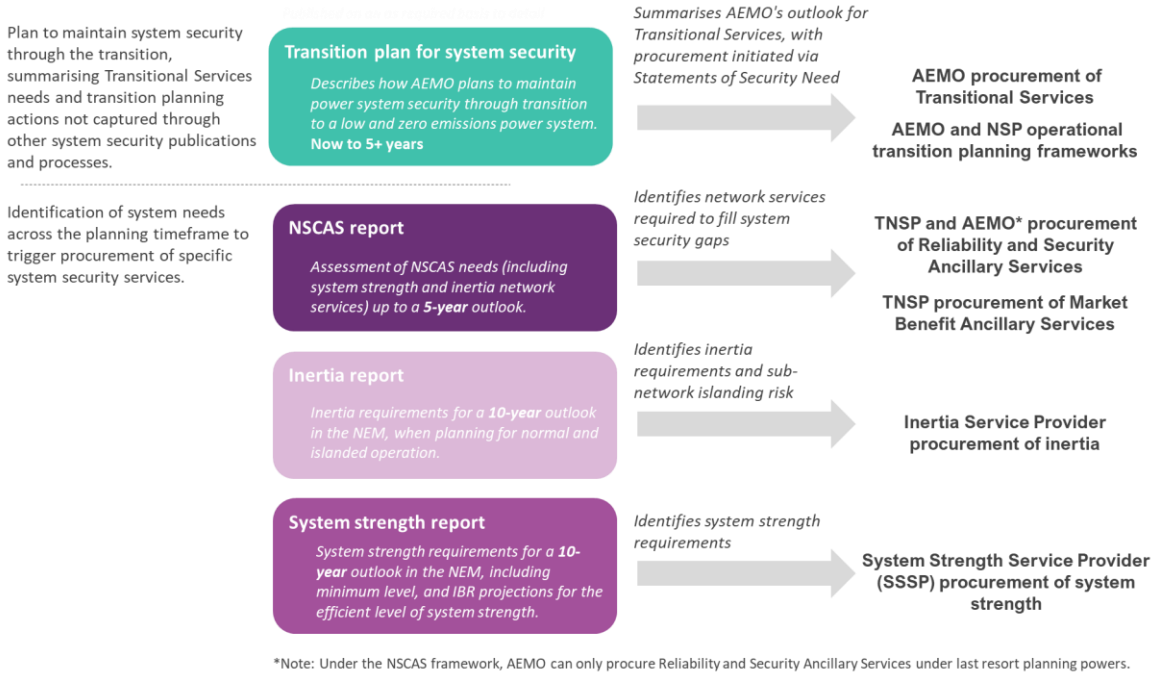
[12] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/2024-system-strength-report.pdf

- the NSCAS Description and Quantity Procedures made under NER 5.20.2[13], and the associated annual NSCAS Report[14], and

Additionally, any statement/s of security need for transitional services (as defined under NER 3.11.11 (b)) are published in accordance with the Transitional Services Guideline[15,16].

The relationships between these processes, and their underlying intents are illustrated in Figure 2.

Figure 2 Relationship between AEMO system security reports and Transition Plan for System Security



It is proposed that the Procedures adopt these same methodologies as far as practical for determining security requirements, adapting them only where appropriate to consider the more nuanced, dynamic or extreme system conditions observed operationally. Table 1 outlines how system security components in the published documents will be implemented in the operational timeframe to establish the minimum system security requirement.

[13] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/nscas-description-and-quantity-procedure-v3-0.pdf

[14] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/2024-nscas-report.pdf

[15] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/ancillary_services/transitional-services/transitional-services-guideline_

[16] An example of a Statement of need can be found at https://aemo.com.au/consultations/tenders/minimum-system-load-transitional-services-for-victoria-and-south-australia

Table 1 Components of minimum system security requirement

Service	Component	How requirement will be implemented in the operational timeframe
Inertia	The *inertia sub-network allocation* for each inertia sub-network, being a portion of the mainland inertia that AEMO considers is required to operate the system securely during normal interconnected operation	Consistent with the methodology and considerations outlined in the Inertia Requirements Methodology, and used to calculate TNSP requirements in the annual Inertia Report[17] These will be adapted for use in operational timeframe through the implementation of system security inertia constraints that reflect current system conditions, and which calculate the resulting level of inertia expected to be required in each region to maintain a secure and satisfactory operating state Information on system security inertia constraints can be found in AEMO's Constraint Formulation Guidelines[18] and Constraint Implementation Guidelines[19] (which are the subject of a separate consultation)
Inertia	The *satisfactory inertia level* for each inertia sub-network, being the minimum level of inertia that AEMO considers is required to maintain the sub-network in a satisfactory operating state when islanded or at credible risk of islanding	
Inertia	The *secure inertia level* for each inertia sub-network, being the minimum level of inertia that AEMO considers is required to maintain the sub-network in a secure operating state when islanded or at credible risk of islanding	
System strength	The *minimum three phase fault level* required at each system strength node that AEMO considers is required to ensure network protection and voltage control systems operate correctly, and that the system remains in a secure operating state [20]	Requirements will generally be consistent with the methodology and considerations outlined in the System Strength Requirements Methodology and which are used to calculate TNSP requirements in the annual System Strength Report[21] TNSP's (system strength service providers) are required to procure sufficient assets and services to ensure that these planning requirements can be met continuously AEMO will operationalise the minimum fault level requirements using a set of constraints that reflect expected system conditions, and which calculate the resulting levels of system strength service expected to be required to maintain a secure operating state TNSPs will provide AEMO with specific limits advice to inform the development of these constraints, to ensure consistency with the modelling and assumptions used by TNSPs in selecting their suite of system strength service Providers AEMO will enable only those Providers necessary to meet any expected gap between these requirements and the levels of system strength delivered by market dispatch outcomes
NSCAS	A NSCAS need to the extent reasonably considered necessary by AEMO to maintain the power system in a secure operating state	Requirements will be calculated consistent with the nature, timing, and magnitude of the corresponding

[17] https://www.aemo.com.au/energy-systems/electricity/national-electricity-market-nem/nem-forecasting-and-planning/system-security-planning

[18] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/congestion-information/2023/constraint-formulation-guidelines-v12---final_1.pdf

[19] https://aemo.com.au/-/media/files/stakeholder_consultation/consultations/nem-consultations/2023/constraints-implementation-guidelines/final-constraint-implementation-guidelines-v3.pdf

[20] Note that the stable voltage waveform component of system strength is not part of the minimum system security requirements, and is calculated/enabled as described in Section 5.

[21] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/2024-system-strength-report.pdf

Service	Component	How requirement will be implemented in the operational timeframe
		NSCAS gap, as declared in AEMO's annual NSCAS Report[22] Based on that same gap declaration, the triggers for enablement will reflect the operational conditions under which the NSCAS gap was identified The specific method of enablement may vary based on the type of security gap, and on the underlying mechanism by which the contracted Provider addresses it
Transitional	The power system security needs and expected duration specified in the statement for transitional services published under NER 3.11.12(a)(2)(i) from time to time, where applicable	As outlined in the relevant Statement of Security Need
Other	Any other power system security requirements that AEMO determines from time to time are necessary to maintain the power system security standards	To be determined based on type of security need being addressed. AEMO or TNSP contract information includes provider's contribution to relevant security need

3.1.1. Security services constraints

System security inertia and system strength constraints are formulated through:

- consultation with industry to adopt the principles outlined in AEMO's Constraint Formulation Guidelines[23]
- TNSP limits advice provided to AEMO in accordance with AEMO's Limit Advice Guidelines[24]

Questions

2. Do you have feedback on the methodologies and reports listed above for establishing minimum system security requirements in the operational timeframe?
3. What other factors do you consider relevant in determining minimum system security requirements?

3.2. System security enablement methodology

The System Security Enablement Methodology must be implemented in accordance with enablement principles under NER 4.4A.4 that can be summarised as follows:

- lowest total cost combination to achieve required outcomes
- enabled as close as practicable to requirement timing and no more than 12 hours ahead

[22] https://www.aemo.com.au/energy-systems/electricity/national-electricity-market-nem/nem-forecasting-and-planning/system-security-planning

[23] https://aemo.com.au/-/media/files/stakeholder_consultation/consultations/nem-consultations/2022/cfg-and-scvpf/final/constraint-formulation-guidelines-v12---final_.pdf - AEMO is undertaking a consultation on these Guidelines to amend and include the new system security inertia and system strength constraints forumlations.

[24] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/congestion-information/2025/limits-advice-guidelines.pdf

- only enabled where, in AEMO's reasonable opinion, the service is required to achieve the minimum system security requirements or the stable voltage waveform requirements
- enabling a system security service for stable voltage waveform requirements:
  - can only be in order to increase inverter-based resources (IBR) and market network service dispatch
  - must avoid adverse effects on power system efficiency or power system emissions.

Section 3.2.1 describes AEMO's proposed enablement processes for the minimum system security requirements and how these processes will ensure system security services are enabled in operational timeframes in accordance with the above enablement principles. Section 3.4 describes AEMO's approach for the stable voltage waveform requirements.

3.2.1. Proposed AEMO enablement processes

The following are the proposed enablement processes for system security services to give effect to the enablement principles above in operational timeframes:

- an automated process to meet the minimum security requirements for system strength and inertia using system security services that align with the agreed contractual structure identified in section 3.3
- a manual process, where appropriate, including for other system security services[25]
- an enablement process for the stable voltage waveform requirements, which is discussed in section 3.4.

Table 2 Proposed enablement processes

Requirements	Service	Proposed Enablement Process
Minimum system security requirements	Inertia	Automated system security services enablement, with a manual process adopted if required as a transitionary and/or fallback arrangement
	System Strength	
	NSCAS	Manual system security services enablement or automated in the security service scheduler if service definition and contract structure permits or if can be automated via alternative AEMO system
	Transitional	
	Other	
Stable voltage waveform requirements	System Strength	Enablement for the stable voltage waveform requirements (see section 3.4)

Automated system security services enablement

The process for automated assessment of gaps in the minimum system security requirements, and enablement to meet any gaps, that relate to inertia and system strength is illustrated in Figure 3 and described in further detail in Table 3.

[25] Consistent with the approach outlined in Table 6.1 of AEMC ISF Rule Final Determintation https://www.aemc.gov.au/sites/default/files/2024-03/ERC0290%20-%20ISF%20final%20determination.pdf

Figure 3 System security enablement process

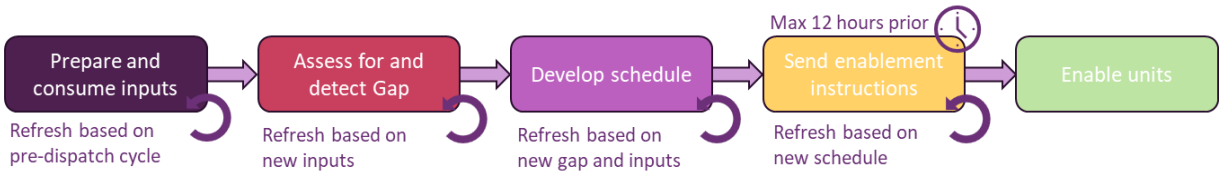
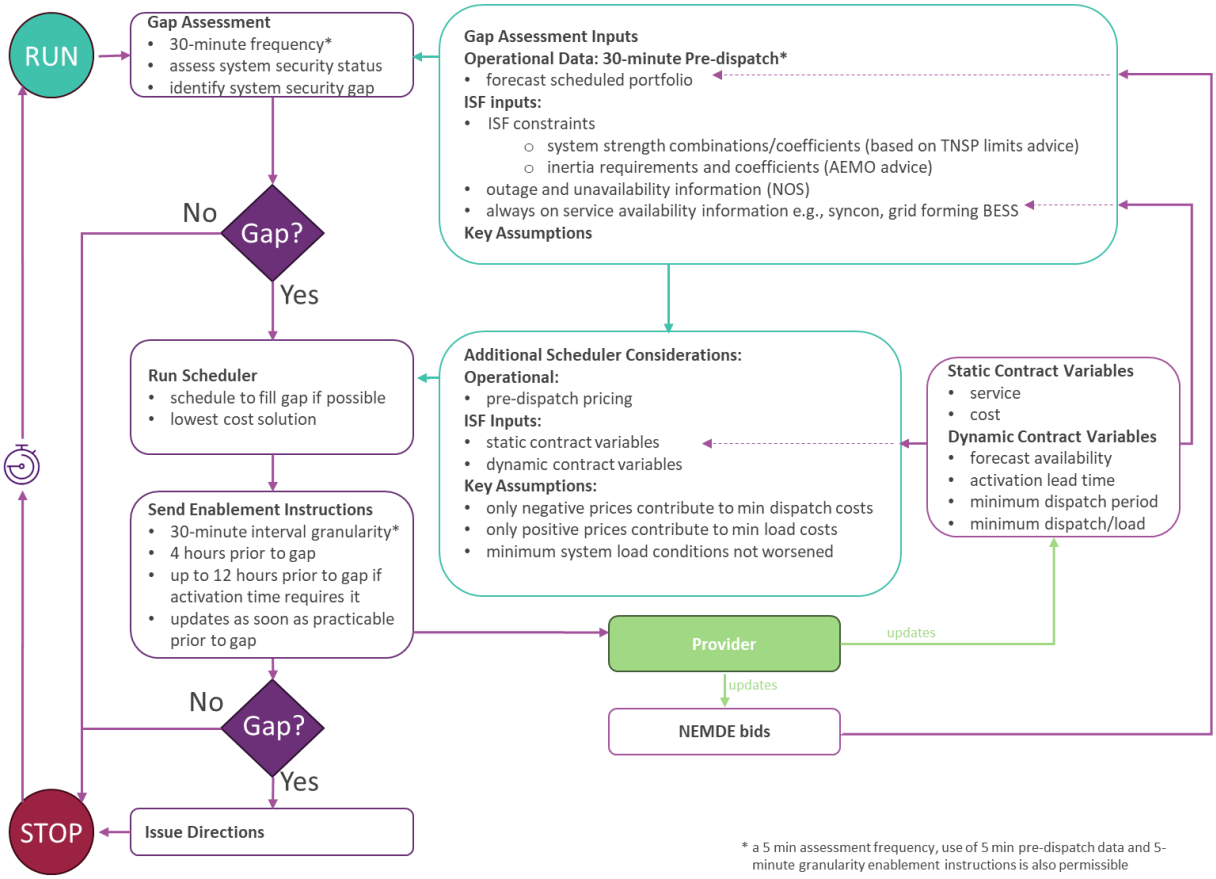


Table 3 Automated enablement process steps

System security enablement step	Detail
Prepare and consume inputs	• Establish minimum system security requirement in accordance with methodology (see section 3.1) • Source inputs from: – TNSP limits and AEMO advice for system strength and inertia – Pre-dispatch information to understand expected portfolio of resources online and inherently providing security services – Network outage scheduler (NOS) to understand line outages, synchronous condenser status and other relevant equipment status – Provider interface for security service operational information including availability
Assess for and detect Gap	• Determine level of system strength and inertia that is expected to be online prior to any security service enablements • For each pre-dispatch period compare minimum system security requirement with anticipated power system security (system strength and inertia) via energy market • If system strength or inertia is not forecast to meet the minimum requirement, identify a shortfall/gap
Develop Schedule	• Retrieve availability, service details (activation lead time, minimum dispatch (where applicable) and service volume) and cost of services that can meet gap • Establish a least cost solution (see section 3.2.23.2.2) for the pre-dispatch timeframe • Rerun process as new data becomes available and predispatch are updated
Send Enablement Instructions	• Send instructions to Providers in accordance with enablement instruction methodology (see section 3.20) • Send enablement instruction 4 (IEI) hours from gap or longer (up to 12 hours ahead) taking account of activation lead time • Update instructions to Providers as required based on latest data and schedule
Enable units	• Providers comply with enablement instructions • Providers update dispatch bids as required • AEMO invokes security service constraints for inclusion in the NEM Dispatch Engine (**NEMDE**) and pre-dispatch

The assumptions and inputs that guide the enablement of units outlined in Table 3 are illustrated as a workflow in Figure 4 and discussed in more detail throughout section 3.2. AEMO is implementing a cycle, for the purpose of gap assessment, scheduling and enablement, linked to the existing pre-dispatch data refresh. For the 2 December 2025 effective date, a 30-minute cycle based on 30-minute pre-dispatch is planned to be implemented, with a view to assessing the benefits of a 5-minute cycle through inclusion of 5-minute pre-dispatch data at a later time.

Figure 4 Overview of assumptions and inputs in the enablement methodology



Manual system security services enablement

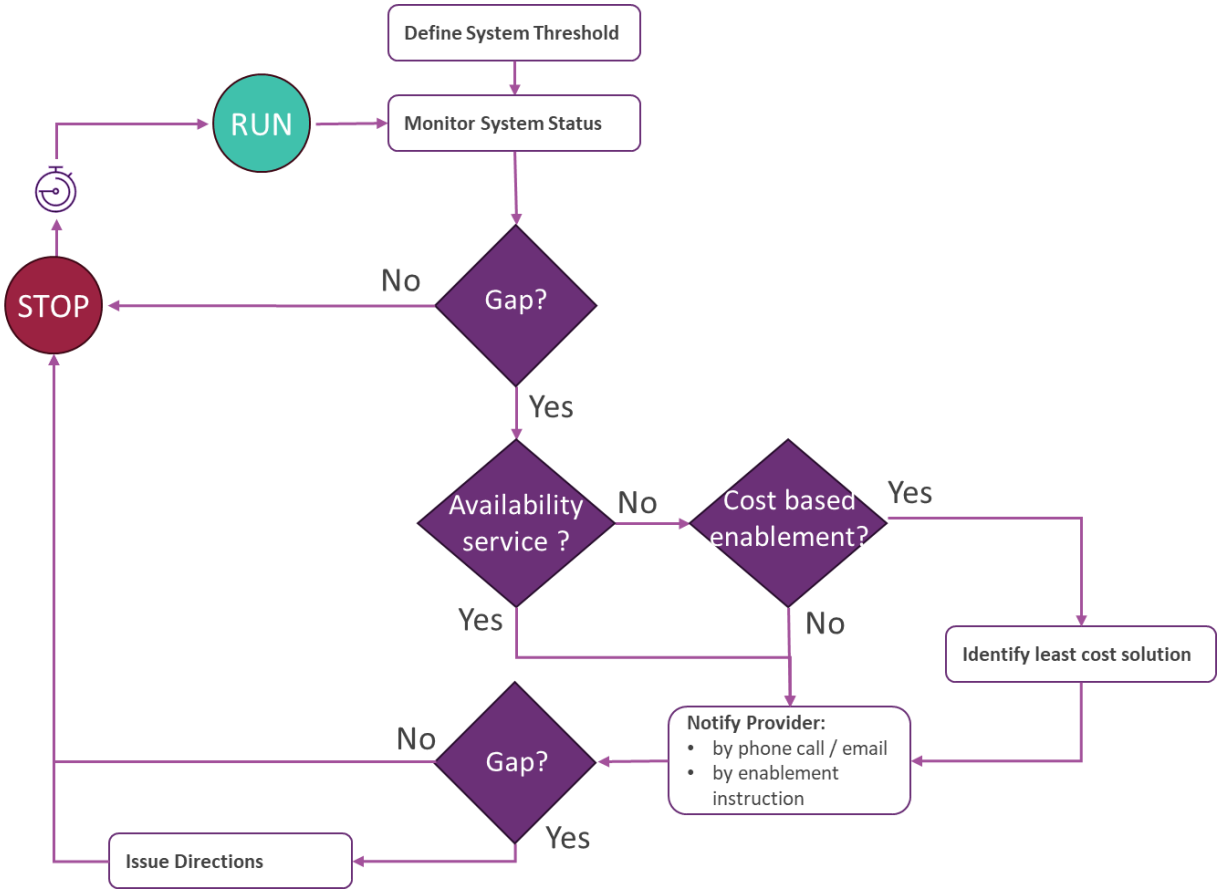
System security services that are not enabled through the automated enablement process system will be managed outside the automated process. The key steps, illustrated in Figure 5, may involve:

1. Definition of the threshold to trigger service enablement.
    - For NSCAS this will be the identified NSCAS gap that must be procured by AEMO as provider of last resort.
    - For transitional services this will be the level published in a statement of need.
2. Monitor the system conditions to identify if the threshold level is not being met (that is, there is a gap) for the forecast operational conditions.
3. Notify Providers that are on availability (ongoing service provision) contracts of potential gap via agreed instruction process.
4. Where appropriate, rank contracts that require enablement by anticipated cost and establish a priority enablement list.
5. Enable service(s) in accordance clause 4.4A.5(b) and cease enablement instruction in accordance with clause 4.4A.5(c) in the manner specified in Section 4.

Where identified under an ancillary services agreement, the requirements set out in Section 3.4.4 'Variable parameters required to be restated' and Section 3.4.5 'Spot market operation and enablement' of the Procedures will apply.

The variety of potential security services requires AEMO to adopt a generalised manual process to be adapted for each specific requirement as it arises. The enablement process for each system security requirement will be established in accordance with the principles outlined in the Procedures. The form of the service and operational thresholds for usage will be published in the relevant documents as specified in Table 1. The manual process may be more or less automated depending on the operational requirements of each security service.

Figure 5 Overview of potential steps in a manual enablement process



AEMO will continue to consider the potential to automate enablement for manually enabled services as the systems are incrementally developed over time. The Procedures have been developed to allow adoption of automation without changes to the Procedures where appropriate. If Procedure changes are required these will be consulted on with stakeholders under NER 8.9.2.

Fall back enablement mechanism

AEMO requires a fall back mechanism in the event that the automatic enablement process malfunctions, fails to fill a gap due to insufficient schedulable security services or creates other issues with a potential impact to power system security. AEMO will continue to exercise reasonable endeavours to meet the enablement principles in these situations, with maintaining power system security given priority.

The fall back process may include AEMO:

- suspending the automatic enablement processes
- canceling erroneous enablement instructions
- amending scheduler inputs and triggering an out-of-cycle scheduling run

- adopting a manual enablement process.

In the event that operational time pressure prevents enablement of security agreements through manual processes, AEMO will revert to issuing directions to ensure power system security.

Ability to resecure in the event of a contingency

AEMO is retaining its current power system operating requirements following implementation of the ISF Rule, as outlined in Section 3.1. AEMO operates, the power system in a secure operating state to the extent practicable, including the ability to return the power system to a secure operating state (resecuring) within 30-minutes following a credible contingency as required under NER 4.2.6.

In the near term and from the effective date of 2 December 2025, AEMO does not expect high volumes of security service contracts to be available in each NEM region for enablement. AEMO is initially developing its enablement processes with this in mind. This means that the automated scheduling process will (by default) schedule security service units for enablement to address a gap, absent automatically enabling/reserving security service units for enablement such that the power system is able to resecure within 30-minutes following a credible contingency. This means that an additional manual process is required, post development of a security schedule, as follows:

- Identify additional security service units that are available for enablement within 30 minutes (and currently not scheduled for enablement)
- When the schedule does not allow for the system to be resecured within 30 minutes, assess the time until gap to determine the best option to meet resecure requirements; being either:
    - Adjusting the security enablement schedule through manual intervention to ensure the power system can resecure within 30 minutes; or
    - Identify suitable directable units to meet resecure requirements and direct as required.

As system development time allows, AEMO proposes that the scheduling process will incorporate functionality to automatically reserve ‘fast start’ security service units for enablement in the event of a contingency. Where insufficient ‘fast start’ units are available for AEMO to resecure in the event of a contingency, AEMO may enable other security service units on a pre-contingent basis to meet resecure requirements, when developing the security schedule. If both of these options are unavailable, AEMO will resort to issuing directions to ensure power system security.

AEMO proposes that the Security Enablement Procedures be developed to accommodate both arrangements described above, and to provide stakeholders transparency of when new system capability allows the latter arrangement to be adopted via its Improving Security Frameworks Industry Go-Live Plan.

Questions

4. Do you agree that the automated and manual enablement processes described will be practical and suitable for the real-time operational requirements of the relevant system security services?
5. What other factors should a fall back mechanism take into account?
6. What other factors should AEMO consider in developing these enablement processes?

3.2.2. Enablement principles

AEMO will use reasonable endeavours to give effect to the enablement principles under NER 4.4A.4. Each enablement principle is examined below.

Lowest system security service cost

The enablement principle under NER 4.4A.4(a) requires AEMO to use reasonable endeavours to enable the lowest total cost combination of system security services.

The two factors that contribute to the cost of enablement of security services are the volume of service required to meet a gap and the cost of services.

Under the automated process, a security service scheduler containing an intertemporal linear programming solver will be developed to resolve minimum system security requirement gaps of system strength and inertia at least cost. It will take into account the amount of services required and provided, activation lead time (dynamic), minimum dispatch (dynamic) and availability (dynamic). Availability payments are not taken into account as these are sunk costs which occur whether an asset is enabled or not.

- AEMO may mitigate the cost of multiple activations for an asset by extending an enablement instruction so that services are provided for periods of time that they are not always required for minimum system security, but overall achieve the lowest cost outcome for when they are required.

Latest available pre-dispatch pricing is proposed be used to estimate the energy revenue associated with enablement of each service, as the energy price cannot be known prior to enablement. See section 3.3 for further information on financial parameters.

Closest system security service enablement time

The enablement principle under NER 4.4A.4(b) requires AEMO to use reasonable endeavours to enable system security services as close as practicable to the relevant trading interval and not more than 12 hours in advance.

All security service enablement processes conducted by AEMO (automatic or manual) will maintain the following two operational requirements:

- AEMO will send enablement instructions to system security services at their activation leadtime, and
- no security services will be issued an enablement instruction greater than 12 hours in advance of the commencement of an identified security need.

For the automated enablement process, AEMO is proposing to:

- commence issuing enablement instructions four hours before the start of a system security gap, or
- to meet the activation lead time if greater than four hours, or
- immediately if a gap is identified to occur in less than four hours

AEMO will issue new or amended instructions if system conditions change:

- as soon as practicable before the start of the new or amended instruction which can include
    - an update to the start time and end time of an enablement

- a cancellation of an enablement (which may involve the payment of any activation payment for which the activation lead time has passed)

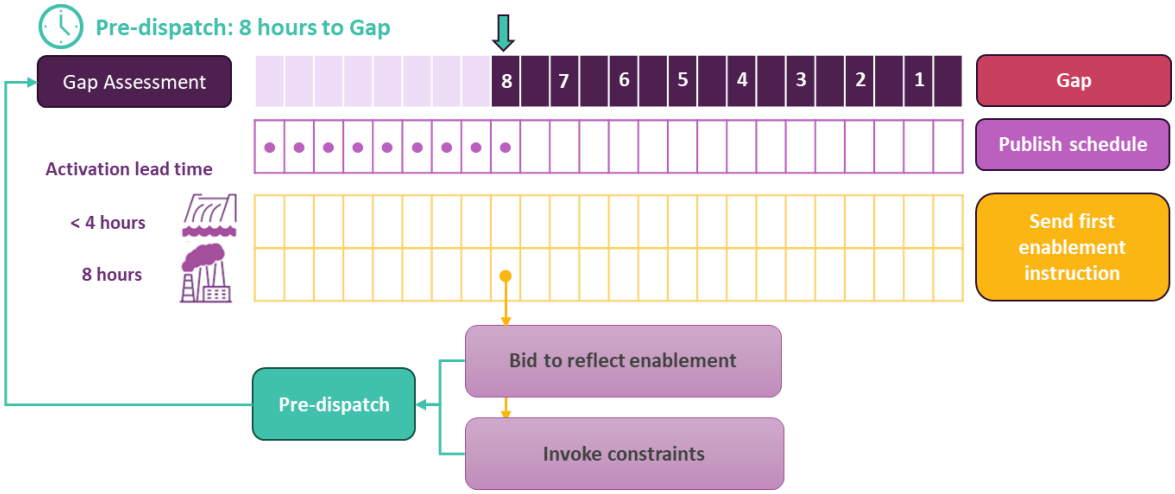
- in the case of a lower cost solution[26] being identified, only if the threshold cost saving for the forecast cost saving is met.

AEMO's approach has been designed to prioritise power system security, increase transparency for stakeholders and minimise short term changes to enablement instructions.

Pre-dispatch will incorporate Provider energy bids and associated constraints (reflecting their minimum dispatch where applicable) ahead of the enablement timeframe (the greater of the four hour window, or the activation (enablement lead). If the system security gap is identified less than four hours in advance then the enablement timeframe will be the time between identification and forecast eventuation of the gap.The proposed timing is illustrated in Figure 6.

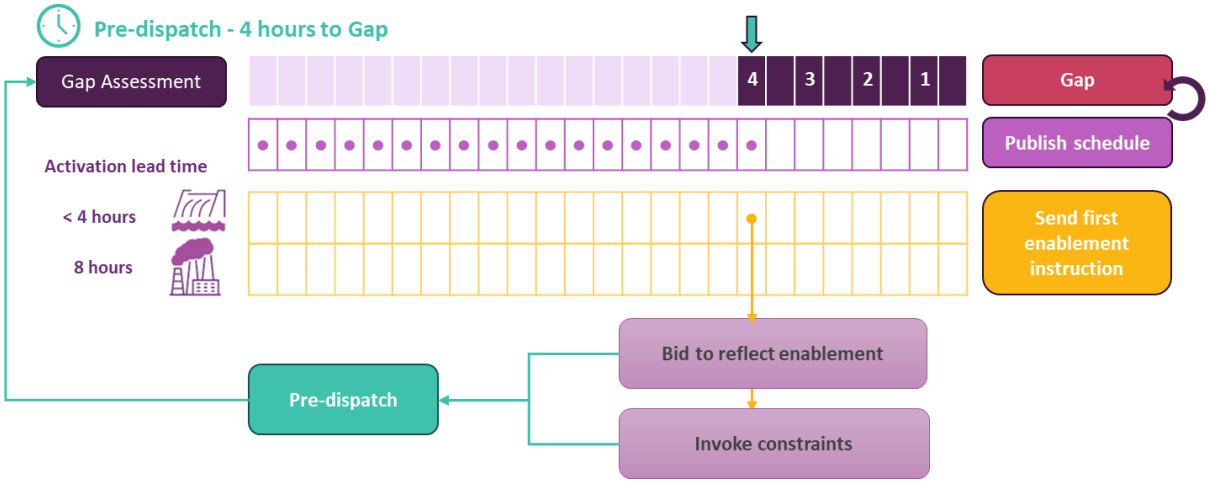
AEMO regards these arrangements to be as close as reasonably practical to the relevant enablement commencement time. These arrangements are required to provide visibility of the security schedule's impact on the electricity market and allows electricity market participants and AEMO's operations to make informed decisions based on pre-dispatch outcomes that include enablement of security services. This approach is intended to minimise the risk that electricity market responses to issuance of enablement instruction/s occur closely prior a relevant dispatch period, and result in a subsequent need to revise the security schedule, thus creating unnecessary instability of electricity market and security enablement outcomes.

Figure 6 Illustration of schedule, enablement and enablement update timings.

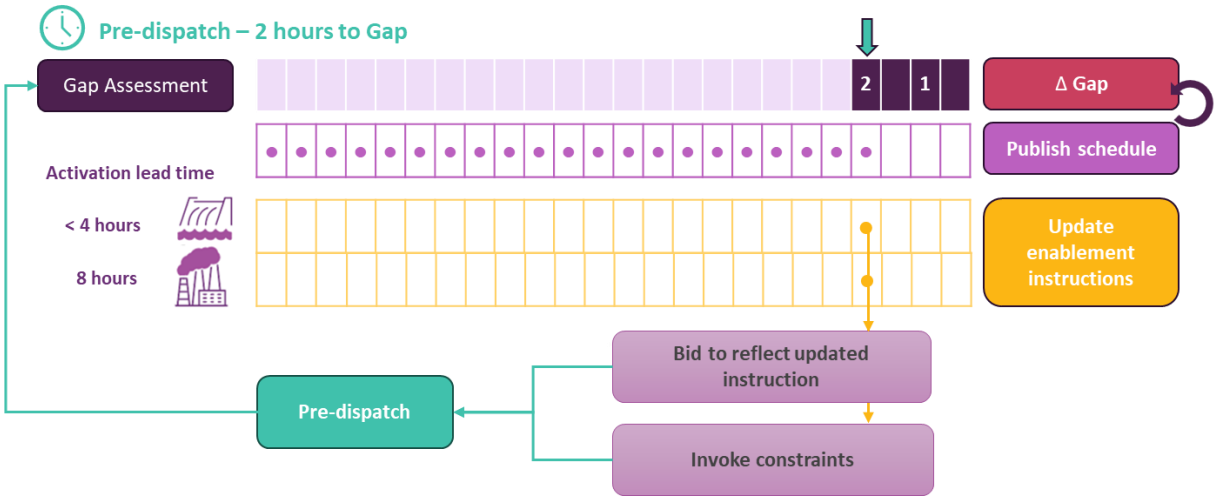


A gap in 8 hours time requires the services of a thermal plant with an 8 hour lead time. The thermal plant is enabled 8 hours prior to gap and bids into NEMDE accordingly

[26] A lower cost solution to meet a gap will ignore sunk costs for enablement if an asset has passed its activation lead time.



The gap, now in 4 hours time, requires the services of plant with lead times less than 4 hours. All remaining enablement instructions are issued and enabled plant bid into NEMDE accordingly.



The gap, now in 2 hours time, has changed in size requiring an update to enablement instructions. All enablement instruction updates are issued and enabled plant bid into NEMDE accordingly

System security service enablement

The enablement principle in NER 4.4A.4(c) requires AEMO to use reasonable endeavours to enable security services only in circumstances where the minimum system security requirements or stable voltage waveform requirements would not be otherwise met.

AEMO will only enable system security services when a gap in the minimum system security requirements or breach of the stable voltage waveform requirements is identified, with the following clarification:

- A recognition that continuous-services or 'always on' contracting arrangements may be the most cost-effective means of provision of some services. In these cases the services will be provided at times when they are, and are not, needed for minimum system security. AEMO will take account of this type of service provision on an 'as available' basis in performing its system security gap assessment.

The size of a system security gap depends on the minimum level of security services required for the operational circumstance (as described in section 3.1) and the levels of system strength and inertia forecast to be online. In

determining this forecast, AEMO must make assumptions on information that is not available to AEMO in predispatch timeframes or at all.

This information and the proposed assumptions are provided in Table 4. These assumptions reflect AEMO's risk based approach to ensure that power system security can be confidently maintained.

Table 4 Key assumptions in determining system security services gap

Issue	Assumption
Dispatch unit identifier (DUID) with multiple physical units Where a DUID has multiple units and a combination of these can be used to meet their energy dispatch target then it is not possible to know in the predispatch timeframe how many units are expected to be operating. This means the level of inertia and system strength expected to be provided by the DUID is not known	• AEMO will assume the worst case scenario; that is, based on the predispatch megawatts (MW), AEMO will assume the combination of units with the least inertia / system strength provision is online to meet the dispatch target
Grid forming batteries AEMO is not able to see if a grid forming battery is in grid forming mode in the pre-dispatch timeframe	• Grid forming batteries are assumed to be providing no inertia or system strength ahead of time, unless they are otherwise contracted or enabled to do so • Where a grid forming battery is unavailable in the Provider interface AEMO will assume it is not providing any services in pre-dispatch
Synchronous condensers It is not possible to know if a private (non- regulated) synchronous condensers are on line or not from predispatch data	• If the synchronous condenser is a Provider, the synchronous condenser operator will provide availability and status information through the Provider interface, unless otherwise agreed with the relevant TNSP and AEMO to report availability via other means. • Where a stand alone synchronous condenser is not a Provider, AEMO will assume the worst case scenario (that it is offline), unless: – it has an arrangement with the TNSP to report outages via Network Outage Scheduler (NOS), in which case AEMO will assume it remains available when not advised otherwise by a TNSP through the NOS or via limits advice; or – its treatment is agreed otherwise between AEMO and the TNSP and is specified in TNSP limits advice • Where a synchronous condenser is owned and operated by a TNSP, the synchronous condenser will be assumed available, unless reported otherwise via NOS
Spot market operation and enablement An enabled asset that is a market scheduled production unit that decides to bid above a minimum dispatch target is moving into "commercial operation" in favour of security service enablement and will cease to be paid under their security service contract for the period which they are operating commercially	• An asset that moves from system service enablement to commercial operation using the same capacity/energy will cease to be paid but will continue to be enabled and must provide the service until the end of the enablement period • This assumption does not apply to assets, such as a battery, which can provide a service without dispatching or consuming energy as a byproduct of enablement i.e. do not have a minimum dispatch target and are not compensated for minimum dispatch through energy revenue payments

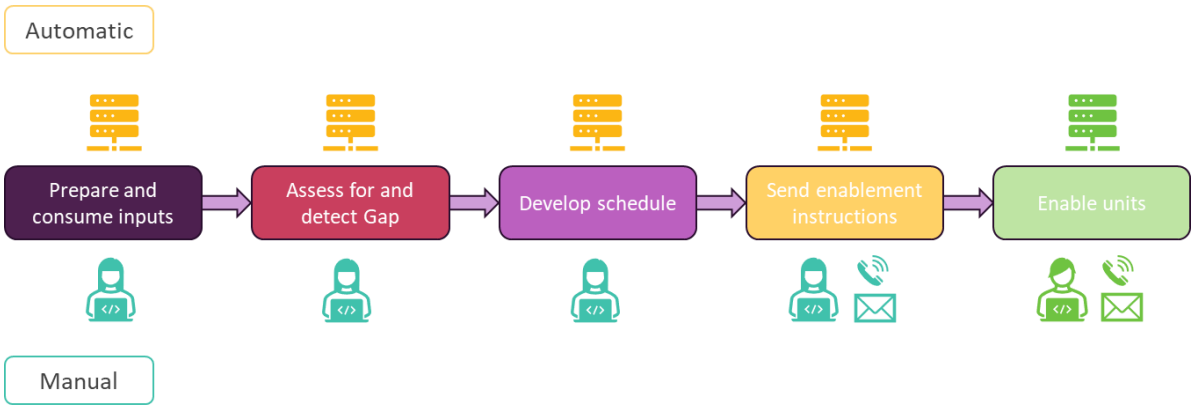
Questions

7. Are there any further concepts that AEMO should consider to give effect to the enablement principles of NER 4.4A.4?
8. Do you agree with the assumptions that AEMO is proposing to use to assess the system security gap through the scheduler? If not, what assumptions would you make and why?
9. Do the timings for enablement instructions and amendments strike a good balance between operational efficiency, transparency and cost efficiency?

3.2.3. Enablement instructions

All Providers must meet security service enablement instructions in the form identified in the Security Enablement Procedures. The enablement instructions will be sent via an automated system for the services that are enabled through the automated enabling process. Services that are assessed through a more manual methodology (see section 3.2) are likely to have a manual process for enablement, as illustrated in Figure 7.

Figure 7 Types of enablement for automatic and manual enablement instructions



Automated enablement

AEMO will develop a new system to allow Providers to submit information regarding their service availability and other operational parameters in their contract that are subject to change. This information will be consumed by the AEMO system performing the gap assessment and scheduling process. Providers are required to update dynamic information as soon as practical to ensure that the latest operational information is available to the scheduler.

Enablement instructions will be issued to Providers separately to energy and frequency control ancillary service dispatch instructions. AEMO is adapting existing interfaces for this purpose. Further detail on the form of enablement instructions will be provided in the next release of the High Level Impact Assessment and during the development of technical specifications. See the ISF program initiative webpage for more details[27].

Manual enablement

Services that are manually enabled will receive enablement instructions in accordance with security service agreement, or as agreed in the relevant ancillary service contract (for example, automated enablement instruction, phone call or email). Where automated enablement mechanisms fail, AEMO will follow the fallback enablement mechanism as outlined in section 3.3 of the Security Enablement Procedure.

Questions

10. Do you agree with the above approach for the provision of enablement instructions?

[27] https://aemo.com.au/initiatives/major-programs/nem-reform-program/nem-reform-program-initiatives/improving-security-frameworks-for-the-energy-transition

3.2.4. Enabling a system security service for stable voltage waveform requirements

AEMO is proposing to implement TNSP limits advice in constraints to meet efficient levels of stable voltage waveform. Further detail is presented in section 3.4.

3.3. Requirements in TNSP system security agreements

AEMO has completed a significant round of engagement with TNSPs in 2024 to develop the Provisional Procedures that contain the requirements in agreements for the provision of security services to be entered into by TNSPs. This early consultation was required to allow TNSPs to progress their negotiation for security services with Providers as soon as practicable.

In determining the initial requirements, AEMO and TNSPs recognised the need for consistency and simplicity. Critical information agreed as required for the security services scheduler is:

- amount of services provided
- activation lead time (dynamic)
- minimum dispatch (dynamic)
- availability (dynamic) and
- cost information.

These requirements inform the way in which AEMO is able to determine and compare the costs of services to meet a system security gap.

Since publication of the Provisional Procedures AEMO has updated its requirements to:

- allow for a minimum run time (see section 3.3.2)
- develop an approach for enablement of a unit or combination of units below the DUID level to provide a service.
- change AEMO's calculation of energy revenue payments to a more appropriate standard assumption for the purpose of determining a least cost schedule.

3.3.1. Fixed and default parameters

The fixed and default parameters are to be defined within the agreement and must be promptly notified to AEMO, including any agreed variations.

Table 5 Fixed and default parameters in AEMO's scheduling system

Category	Requirement	Description
Name and type of asset	• Outline the assets and technology providing the service. • Outline existing NEM registration details. • If an agreement involves an asset with multiple units, each unit should be separately identified List any specifications that are relevant to AEMO's *enablement* of the asset, e.g. when enabled a portion of the asset's energy storage capacity is withheld	• *Connection point* • DUID or unit (if applicable) • *Registration* status, e.g.: *Scheduled* / *market* (if applicable)

Category	Requirement	Description
Services	• *System security service*(s) provided by the asset/s at an individual unit/asset level, e.g. fault current, inertia • An asset must be capable of continuous service provision for at least 2 hours Details of all services that the asset provides when it is enabled regardless whether contracted to provide that service or not	• Quantity and form, e.g. Unit or Asset 1: – X megavolt-amperes (MVA) fault current, – Y megawatt-seconds (MWs) of *inertia*, – participation in a minimum secure commitment configuration
Auxiliary load	For units that are not generating units, scheduled loads or bidirectional unit technologies, expected load consumed when providing service. E.g. synchronous condensers	• Megawatts (MW)
Default activation lead time	• The expected maximum lead time for the *system security service* to be *enabled* from a non-operational state. This will be adjustable in real time	• Defined in hours and minutes. Less than 5 minutes can be stated as zero – Adjustable in real time for physical reasons • ISF Rule prevents AEMO from *enabling* a *security services* asset where the activation lead time is more than 12 hours – If the activation lead time is more than 12 hours the service will be considered unavailable for scheduling and *enablement* • AEMO acknowledges that a *security services* asset may have different activation lead times for different services. Where this is the case the applicable activation lead time for each service should be specified – Must be consistent for units/combinations of units that provide a service in a DUID
Default minimum dispatch	• Minimum stable level of energy dispatch (in absolute terms) required to provide the system security service for a generating unit, scheduled load or bi-directional unit, if applicable	• MW – Adjustable in real time for physical reasons • Will not have usage payment consequences • Will have energy revenue transfer consequences that *AEMO* will take into account in scheduling and *enablement*
Minimum run time	• The expected minimum run time for the system security service once enabled, if applicable	• Hours • Will have usage payment and energy revenue implications • An example is a thermal plant that must run for technical/operational, reasons for a number of hours

Unit or unit combination level enablement within a DUID

AEMO will prioritise the ability to enable at a DUID level for December 2025 and allow for improvement of our security service enablement processes for multiple unit DUIDs as development time allows. AEMO's approach does not restrict TNSP from entering into contracts with multiple unit DUIDs. AEMO will seek to agree appropriate enablement arrangements through the contract approval process to ensure data is provided to AEMO that aligns with the security service enablement processes as they evolve. To cater for the December 2025 and future state a TNSP must adhere to the following guardrails which are proposed to manage the transition to some form of unit level enablement and balance cost efficiency with simplicity:

- DUID based Provider interface information (for December 2025)
- Each unit (for later implementation):
  - is indicated in the Provider interface as available or not available (cannot be partially available)

- is represented by a fixed minimum dispatch (MW)
- has a uniform cost of service across all units (activation, usage)
- has a uniform level of service across all units (MWs, MVA)

3.3.2. Cost structure

The cost structures proposed in the determination of the least cost solution are summarised in Table 6.

Table 6 Financial parameters associated with enablement

Category	Definition	Summary Description
Usage payment	The payment, stated on a per hour basis, that the Provider will receive from the TNSP when the service is enabled	• Dollars per hour of service operation • Usage payments are not payable during the activation lead time
Activation payment	Activation payments (if relevant) are made when a security service asset performs a physical start from a previously inactive state as a result of AEMO selecting the security service to be enabled	• Fixed payment in dollars • If the instruction is cancelled before the activation period no activation payment is payable
Energy revenue	Energy Revenue ($) is the transfer of revenue from the sale of electricity on the spot market ((negative) to the TNSP resulting from the Provider being enabled at Minimum Dispatch or Auxiliary load (if applicable)	• Pass through of negative Energy Revenue to the Provider associated with the Minimum Dispatch (where relevant) or auxiliary load (e.g. that associated with a synchronous condenser)

The payment categories and cost structures should allow TNSPs to provide to AEMO an adequate approximation to the costs of their actual contracts. It is not intended that the categories consider every nuance in a TNSP negotiated contract as this would make the system too complex. Instead of strict requirements, AEMO considers that TNSPs should have sufficient flexibility to conduct commercial negotiations on system security service contract specifications.

System strength and inertia services from one asset

If an asset is capable of being enabled for more than one service there must be a single cost associated with bringing that unit online for security services provision. Contracts must be structured to avoid a different cost for a different service. If a unit is on it will be providing both services, it will be enabled for one and providing the other as a byproduct of enablement. This will:

- avoid paying twice for an enablement instruction to be on line
- simplify security service constraints.

If an asset is contracted for one service but able to provide another then the contract must require that the level of the uncontracted service that the asset will provide as a byproduct of enablement is provided to AEMO. This is to allow an accurate determination of any gap following enablement of the contracted service.

Activation payments and minimum run time

In the Security Enablement Procedure, AEMO has included minimum run times as an optional field in security service contracts. Typically a contract with a minimum run time will include the activation cost, the usage cost and revenue payment for the asset's minimum dispatch. However, given the complexity of implementing minimum run times, it may not be practical to implement a cost determination that includes these three cost

aspects or the minimum run time into an automated enablement process in the December 2025 ISF Rule implementation.

If this is the case, AEMO will, as part of its approval process of arrangements necessary for AEMO to give the instructions under NER 4.3.4(d)(4), 5.20B.6(e) and 5.20C.4(e), require the TNSP to agree to an adjusted activation payment for a contract with a minimum run time to approximate the total cost of enablement i.e., the activation payment in this context will be the TNSP's best estimate of the activation cost, usage cost and energy revenue payments for each enablement up to the minimum run time. In agreeing such an adjusted activation payment, AEMO will seek to ensure the cost of enabling such a contract is not underestimated in its scheduling process. This value will be used to represent the cost of enablement in the automated process.

Following a more complete implementation of minimum run times in the automatic enablement process AEMO will reset the activation cost, usage cost, and energy revenue payments accordingly, such that the scheduler explicitly estimates costs of enabling a unit with a minimum run time.

Modes of operation

AEMO has considered the complexity of catering for different modes of operation from an asset that result in different levels of service provision. For example, a generator operating in syncon mode or generator mode could technically provide different levels of inertia and system strength. AEMO does not consider implementation of different modes practical or necessary by December 2025. AEMO will further assess the need for modes in consultation with TNSPs and stakeholders to determine if it is required in the ultimate target state for the automatic enablement process.

For December 2025 AEMO will, where a contract allows for two modes of operation, assume the mode of operation with the lowest volume of system strength and inertia and apply a payment assumption that corresponds to that mode in its automated enablement process.

Post December 2025 AEMO will work towards a solution that caters for both modes if it is determined this is required. This will require Providers to provide availability information for each mode separately and a mutually exclusive enablement of the mode that allows for the lowest cost schedule to meet a security services gap. Accordingly a TNSP that wishes to contract for two modes of operation must require service volumes and payment amounts that reflect each mode in accordance with the minimum requirements as if they were two separate services from two separate assets.

Energy revenue

AEMO is proposing an assumption for energy revenue costs that meets the principle that costs of security service enablement should not be underestimated when assessing the lowest cost enablement solution.

Energy revenue is used to compensate a Provider with a minimum dispatch amount for energy costs where energy is consumed or dispatched at the spot price in order to provide the enabled service. These costs need to be catered for in any automated enablement solution, as energy revenue can be negative due to low prices for producers of energy and high for consumers of energy, creating significant cost for service provision. If AEMO were to ignore energy revenue then the calculated cost of enablement in the automated enablement solution could be significantly lower than the actual costs.

AEMO recognises there are various forms of calculation of energy revenue that TNSPs and counterparties could agree through contract negotiations and does not wish to limit a TNSP's ability to offer alternative contract arrangements. However, it is not possible for the automatic enablement process to cater for all energy revenue contractual arrangements. For the least cost enablement assessment, AEMO will assume one uniform

calculation across all agreements for energy revenue, to ensure that the cost of enabling such services is not underestimated.

AEMO is proposing an alternative to the assumption in the provisional procedure as a calculation for this consultation. The form of the energy revenue calculation can have undesired impacts and incentives. AEMO's prototyping work has shown that the formulation of full energy cost pass through assumed in the provisional procedure can result in:

- inappropriate prioritisation of thermal units where there are positive spot prices in pre-dispatch based on pass through to TNSPs; this may not be the case represented by the TNSP's contract with the Provider, or
- a negative cost of enabling when there are positive spot prices in pre-dispatch resulting in the enablement of contracts even when there is no gap; this issue would need to be addressed through greater complexity in the solver.

Having considered the impact on the performance of the scheduling solution and the incentives that may arise AEMO is proposing to assume payment to a Provider of any negative revenue price based on pre-dispatch pricing. This takes into account the following:

- avoids perverse incentives in the solution by creating an outcome that creates a negative enablement cost (payment from the Provider to TNSP or AEMO) and may materially distort market outcomes
- captures fundamental AEMO concern in not underestimating costs of enabling a service
- allows time for AEMO to assess the automatic enablement process performance over time and determine if another option will provide material improvements in meeting a least cost solution.

Should implementation of this option of the above calculation with pre-dispatch pricing not be possible by 2 December 2025, AEMO is proposing to adopt an option that assumes the value of energy revenue based on the market floor price as an interim backstop.

These energy revenue costs are not applied to Providers who are able to provide services without a minimum dispatch. Batteries are assumed to provide the service without a minimum energy target and the negotiated usage payment should cover their marginal cost of enablement.

Questions

11. Do you agree with AEMO's guardrails to allow units within a DUID to provide a service?
12. Do you agree with AEMO's approach to minimum run times until the automated process is able to take these into account?
13. Do you agree with AEMO's approach to dual modes of operation until the automated process is able, or required, to take these into account?
14. Do you agree with AEMO's approach to energy revenue assumptions for the purpose of a least cost enablement solution?

3.4. Stable voltage waveform requirements

The stable voltage waveform requirements as defined in NER 4.4A.1(b) are intended to support IBR resources that would be dispatched if not constrained for system strength reasons. These requirements are sometimes known as the efficient level of stable voltage waveform. AEMO may enable system strength services to achieve and maintain the stable voltage waveform requirements.

The ISF Rule provides AEMO with the ability to schedule for stable voltage waveform under conditions set out in 4.4A.4(d), namely:

> *(1) only enable a quantity of system strength services that is reasonably necessary to achieve stable voltage waveforms for the level and type of inverter based resources and market network service facilities that AEMO projects could be dispatched in the relevant trading interval; and*
>
> *(2) not enable a system strength production unit if enabling that unit would result in significant adverse effects on power system efficiency or power system emissions*

Achieving and maintaining the stable voltage waveform requirements using system strength services is a new operational process with no existing NEM mechanisms that can be leveraged to meet this obligation and limited theoretical development to draw upon.

3.4.1. Linkage to the Efficient management of system strength on the power system rule change

Due to a requirement for existing IBR connections to self-remediate their system strength requirements, there is no existing arrangement whereby system strength agreements are enabled to support IBR dispatch. Accordingly, current instances of system strength impacts limiting IBR are infrequent and/or isolated. System strength limits advice provided by TNSPs does not generally put limitation on IBR dispatch based on unit combinations in system normal conditions[28]. AEMO's recent analysis has identified that system strength currently represents less than 4% of all IBR curtailment.

The introduction of the Efficient management of system strength on the power system rule change[29] creates three mechanisms for connecting IBR to remediate their system strength impact:

- central remediation that requires the connecting IBR to pay the TNSP for centrally procured system strength services to support their dispatch; or
- a system strength remediation scheme behind the IBR connection point or
- a system strength remediation scheme on the network funded by the IBR connecting party (system strength connection works).

AEMO is proposing that an automated enablement process for stable voltage waveform will consider the requirement to enable services that have been procured by TNSPs and paid for by IBR connecting parties to centrally remediate IBR that would be otherwise dispatch-limited as a result of system strength impacts.

3.4.2. Proposed approach and timing

In circumstances where enablement of system strength services is required to be enabled to support IBR dispatch (for IBR units that have elected to pay the central system strength charge), AEMO expects that TNSPs

[28] There is a scenario in Queensland that is an exception to this statement.

[29] https://www.aemc.gov.au/rule-changes/efficient-management-system-strength-power-system

will provide limits advice. This advice will include the relationship of system strength services procured to support dispatch of specific IBR units. AEMO intends to use this advice to enable in accordance with the enablement principles and power system conditions.

AEMO's understanding from TNSP discussions to date is that AEMO should have such an automated enablement process in place by July 2026, based on:

- connection timing of IBR that have elected to pay for centrally procured system strength services; and
- a need for AEMO to enable system strength services in order to deliver this service;

AEMO intends to consult on subsequent amendments to this Procedure in the lead up to this time, to further specify its methodology for enablement for stable voltage waveform from mid-2026 onwards. A key focus area for specifying this methodology will be identifying a practicable solution that is reasonably achievable within the timeframe.

For the purpose of this consultation and in relation to the time period from 2 December 2025 until 1 July 2026 AEMO is proposing:

- continuing engagement with TNSPs to ensure enablement arrangements are in place, should a need arise before July 2026 where system strength services should be considered for enablement to meet the stable voltage waveform requirement, subject to the conditions set out in NER 4.4A.4. If required enablement is likely to be a manual process as closely aligned as possible to the process detailed in section 3.2.1.
- security service arrangements that include continuous service provision (for example, TNSPs constructing (or contracting with) synchronous condensers to meet system strength obligations) could address any near-term need for enablement to meet the stable voltage waveform requirement prior to July 2026.
- TNSP delegation will be considered to meet stable voltage waveform requirements where requested, appropriate and readily separable from scheduling for the minimum system security requirement.

Questions

15. Do you agree with AEMO's approach to maintaining the stable voltage waveform for December 2025?
16. Would you be interested in attending pre-consultation information sessions and/or workshops to understand AEMO's analysis to date of potential automated scheduling processes; and to workshop practicable solutions for scheduling to meet the stable voltage waveform requirement in an automated process from 1 July 2026?

4. Enablement delegation

AEMO is conscious that in some instances it may be more efficient for a TNSP to meet the obligations of the ISF Rule and manage its own system security contracts.

Clause 4.3.3 of the NER allows AEMO to delegate some or all of its rights, functions and obligations under Chapter 4 of the NER to an agent or delegate. Clauses 3.11.3(b2), 5.20B.6(b2) and 5.20C.4(b2) of the NER specifically recognise that AEMO may agree to a TNSP *enabling system strength services* or *inertia network services.*

AEMO considers that in certain, limited circumstances, TNSPs may be in a position to meet the requirements of the ISF Rule for enablement, including where existing contractual arrangements and enablement processes are already established. In these circumstances, AEMO will engage with the TNSP to determine if it would be more efficient and operationally practicable to retain the current TNSP arrangements.

AEMO has set out conditions in the Security Enablements Procedure that need to be met in order to allow for this possibility. The conditions for delegating enablement to a TNSP are:

- the relevant TNSP must have, or agree to have, appropriate processes and operational protocols in place for enabling system security services under contracts in alignment with the ISF Rule; and
- the relevant TNSP's contracts and enablement process demonstrates to AEMO's satisfaction that TNSP enablement will be no less efficient than AEMO enablement, and
- AEMO is satisfied that TNSP enablement is an efficient outcome for the market.

If these conditions are met, AEMO may choose to delegate all, or a subset of, system security service enablement to a TNSP. Examples may include but are not limited to:

- AEMO may retain enablement responsibility for system security services to meet the minimum security requirements, but agree that the relevant TNSP enable certain system security services to meet the stable voltage waveform requirements.
- AEMO may agree with the relevant TNSP that a particular system security service agreement is most appropriately or efficiently managed by delegating enablement to the TNSP.

Questions

17. Do you agree with the principles that AEMO is proposing when considering who is best placed to enable system security services under the ISF Rule? If not, what principles do you consider should be applied?

5. Managing operational parameters

AEMO recognises that the Procedures includes parameters which are configurable and may, as the impact and operation of security services becomes better understood, benefit from amendment. For example,

- Threshold cost saving for implementing a lower cost solution within four hour enablement window, currently proposed as $50,000.
- Standard lead time for enablement instructions, the initial enablement instruction (IEI) hours, currently proposed as 4 hours. This applies unless a system security gap appears less than IEI hours ahead.

These variables are defiin the procedures but adopted in this consultation paper for illustrative purposes. AEMO is investigating the potential to establish these parameters in a separate guidance document outside of the Security Enablement Procedure to create agility in the change process, based on guiding principles set out in the procedure.

6. Consequential procedure changes

Table 7 identifies the key changes proposed to be made to align existing procedures with the Security Enablement Procedures and ISF Rule.

Proposed changes to procedures that are consequential from the Security Enablement Procedure are outlined in Table 7. AEMO will provide marked-up versions in stage 2 of consultation. The changes are expected to be minor in nature to ensure consistency with the Security Enablement Procedures and provide transparency to stakeholders for feedback.

Table 7 Consequential procedure changes

Procedure	Details of proposed updates
SO_OP_3708 **Non-market Ancillary Services**	• Changes to reporting requirements • Define NSCAS and align definitions relating to system strength security services in this procedure to Security Enablement Procedures • Include clause 3.11.6(0a) to define what SO_OP_3708 includes and what Security Enablement Procedures include (and clarify this is not required for TNSPs)
SO_OP_3704 **Pre-Dispatch Procedure**	• Expanded description of the use of pre-dispatch in identifying system security shortfalls in the Overview section • Removal of the sentence stating AEMO has no control of the level of rebidding in the Rebidding section
Spot market operations timetable	• Add the next-day reporting of enabled system security services to the Market Information section, as required under NER 4.4A.7(a)
SO_OP_3718 **Outage Assessment**	• Outage assessment process to consider availability of system security services. AEMO will include an explanation that an outage is unlikely to proceed if there are insufficient system security services available to maintain power system security
SO_OP_3715 **Power System Security Guidelines**	• Include enablement of system security services as one of the options for managing secure and satisfactory power system limits

The following items are for noting in relation to the above table:

- SO_OP_3704 is included above for transparency and is not required to be consulted on under NER 8.9.
- SO_OP_3705 is not included in the above list as changes will be undertaken as a separate consultation.
- SO_OP_3707 (Directions and Clause 4.8.9 Instructions) was updated mid-2024 to reflect the enhanced directions reporting required under the ISF rule change. AEMO has reviewed whether any further changes are required in alignment with the Security Enablement Procedures and has concluded that no further changes are required.

Questions

18. Are there any other consequential changes that you believe need to be addressed in AEMO's procedures?

7. Proposed effective date

The proposed effective date of the Security Enablement Procedures is 31 August 2025, aligned with the date by which AEMO must publish these procedures under NER 11.168.2.

8. Summary of issues for consultation

The Security Enablement Procedures are introduced by the ISF Rule. AEMO proposes content for the Security Enablement Procedures considering:

- alignment with existing system security methodologies and reports
- the need to automate the process where efficient to do so
- the requirements for content under the ISF Rule, and
- the tight implementation timeframe for delivery by 2 December 2025.

Submissions may be made on any matter relating to the proposal discussion in this consultation paper. AEMO would welcome comment and feedback on the following matters:

Section	Questions
1.1. Register for the upcoming public forum	1. What specific areas would you like more indepth briefings from AEMO on?
3.1. Minimum system security requirements methodology	2. Do you have feedback on the methodologies and reports listed above for establishing minimum system security requirements in the operational timeframe? 3. What other factors do you consider relevant in determining minimum system security requirements?
3.2. System security enablement methodology	4. Do you agree that the automated and manual enablement processes described will be practical and suitable for the real-time operational requirements of the relevant system security services? 5. What other factors should a fall back mechanism take into account? 6. What other factors should AEMO consider in developing these enablement processes?
3.2.2. Enablement principles	7. Are there any further concepts that AEMO should consider to give effect to the enablement principles of NER 4.4A.4? 8. Do you agree with the assumptions that AEMO is proposing to use to assess the system security gap through the scheduler? If not, what assumptions would you make and why? 9. Do the timings for enablement instructions and amendments strike a good balance between operational efficiency, transparency and cost efficiency?
3.2.3. Enablement instructions	10. Do you agree with the approach for the provision of enablement instructions?
3.3. Requirements in TNSP system security agreements	11. Do you agree with AEMO's guardrails to allow units within a DUID to provide a service?

Section	Questions
	12. Do you agree with AEMO's approach to minimum run times until the automated process is able to take these into account? 13. Do you agree with AEMO's approach to dual modes of operation until the automated process is able, or required, to take these into account? 14. Do you agree with AEMO's approach to energy revenue assumptions for the purpose of a least cost enablement solution?
3.4. Stable voltage waveform requirements	15. Do you agree with AEMO's approach to maintaining the stable voltage waveform for December 2025? 16. Would you be interested in attending pre-consultation information sessions and/or workshops to understand AEMO's analysis to date of potential automated scheduling processes; and to workshop practicable solutions for scheduling to meet the stable voltage waveform requirement in an automated process from 1 July 2026?
4. Enablement delegation	17. Do you agree with the principles that AEMO is proposing when considering who is best placed to enable system security services under the ISF Rule? If not, what principles do you consider should be applied?
6. Consequential procedure changes	18. Are there any other consequential changes that you believe need to be addressed in AEMO's procedures?

Appendix A. Glossary

Term or acronym	Meaning
AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
Constraint Formulation Guidelines	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/congestion-information/2023/constraint-formulation-guidelines-v12---final_1.pdf
Constraint Implementation Guidelines	https://aemo.com.au/-/media/files/stakeholder_consultation/consultations/nem-consultations/2023/constraints-implementation-guidelines/final-constraint-implementation-guidelines-v3.pdf
IBR	inverter-based resources
Inertia Requirements Methodology	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/inertia-requirements-methodology-v2-0.pdf
Inertia Report	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/2024-inertia-report.pdf
Initial Enablement Instruction (IEI)	The standard number of hours prior to a security service gap that an asset which does not have an activation lead time greater than the IEI is sent an enablement instruction
ISF Rule	National Electricity Amendment (Improving security frameworks for the energy transition) Rule 2024
Limit Advice Guidelines	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/congestion-information/2025/limits-advice-guidelines.pdf
NEMDE	NEM Dispatch Engine
NEO	National electricity objective
NER	National Electricity Rules
NCAS Description and Quantity Procedure	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/nscas-description-and-quantity-procedure-v3-0.pdf
NSCAS Report	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/2024-nscas-report.pdf
NOS	Network outage scheduler
Procedures	Security Enablement Procedures
Proposal	This consultation paper and the draft Procedures that accompany it
Provider	Provider of system security services (a TNSP or a third party service provider procured by TNSP or AEMO)
Provisional Procedures	Provisional Security Enablement Procedures
System strength requirements methodology	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system-strength-requirements/system-strength-requirements-methodology.pdf
System Strength Report	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/system_security_planning/2024-system-strength-report.pdf
TNSP	transmisison network service provider

Term or acronym	Meaning
Transitional Services Guideline	https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/ancillary_services/transitional-services/transitional-services-guideline_