Security Enablement Procedures

Prepared by:	AEMO Operations
Document ref:	SO_OP_3720
Version:	1.2
Effective date:	31 August 2025
Status:	DRAFT

Approved for distribution and use by:

Approved by:	Michael Gatt
Title:	Executive General Manager Operations
Date:	13/06/2025

Contents

Current version release details 3

1. Introduction 4

1.1. Purpose and scope 4

2. Minimum System Security Requirements 7

3. System Security Services Enablement 10

3.1. Automated system security services enablement 10

3.2. Manual system security services enablement 12

3.3. Fallback enablement mechanism 13

3.4. Enablement principles 14

3.5. Form of System Security Enablement Instructions 17

4. TNSP System Security Services Agreements 20

4.1. General agreement structure 20

4.2. Defining service provision 20

4.3. Financial structure 23

4.4. General requirements 25

5. Stable Voltage Waveform Requirements 27

5.1. Enablement for the stable voltage waveform requirement 27

6. Enablement Delegation 29

Version release history 30

Tables

Table 1 Implementing minimum system security requirements in the operational timeframe 8

Table 2 Enablement Processes 10

Table 3 Automated enablement process steps 11

Table 4 Key assumptions in determining a system security services gap 15

Table 5 Fixed and default parameters in AEMO's scheduling system 21

Table 6 Variable operational parameters 22

Table 7 Financial parameters in AEMO's scheduling system 25

Figures

Figure 1 Relationship between Security Enablement Procedures and other key operational documents 6

Figure 2 High Level System Security Enablement Process 11

Figure 3 Potential Assumptions and Inputs in the Enablement Process 12

Figure 4 Steps in Manual Enablement Process 13

Figure 5 Financial structure 23

Current version release details

Version	Effective date	Summary of changes
1.1	31 August 2025	Draft version for consultation
1.2	31 August 2025	Draft version for consultation

Note: There is a full version history at the end of this document.

1. Introduction

1.1. Purpose and scope

These are the Security Enablement Procedures made under clause 4.4A.6(a) of the National Electricity Rules (NER) (Procedures).

These Procedures have effect only for the purposes set out in the NER. The NER and the National Electricity Law prevail over these Procedures to the extent of any inconsistency.

These Procedures describe:

- the methodologies for:
  - determining the *minimum system security requirements* in accordance with NER 4.4A.3
  - enabling *system security services* in accordance with the enablement principles in NER 4.4A.4
- how AEMO determines the level of *stable voltage waveform requirements* in NER 4.4A.1(b) and the approach to enablement of *system security services* to this level.
- the requirements to be included in agreements for the provision of *system security services* entered by TNSPs.

1.1.1. Glossary

Terms defined in the National Electricity Law and the NER have the same meanings in these Procedures unless otherwise specified in this clause.

Terms defined in the NER are intended to be identified in these Procedures by italicising them, but failure to italicise a defined term does not affect its meaning

In addition, the words, phrases and abbreviations in the table below have the meanings set out opposite them when used in these Procedures.

Term	Definition
Activation lead time	The time required for a *security service* asset to become *enabled* for a *system security service*/s after receiving an instruction from AEMO for *enablement*.
Activation payment	A payment to reflect the Provider's cost of commencing operation from a previously inactive state.
Activation period	The period (corresponding to the activation lead time) between a *security service* asset being instructed for *enablement* and being *enabled* to provide a *system security service*.
AEMO	*Australian Energy Market Operator Limited*
Available	A *security service* asset is available if it is capable of providing *system security services* after its activation period if instructed by AEMO to do so or it is paid an always on availability payment and not enabled, e.g., grid forming battery in grid forming mode.
Availability payment	A payment that reflects a Provider's fixed costs for maintaining the availability of the *system security service.*
EMMS	the AEMO Electricity Market Management System
Enabled	As provided in the NER, a *system security service* is *enabled* when a *security service* asset provides the service in accordance with AEMO's instructions. A service commences *enablement* after the activation period ends.
Enablement period	The period over which a *security service* asset is instructed by AEMO to provide a *system security service*/s.

Term	Definition
DUID	*Dispatchable unit identifier*
Energy revenue	The transfer from the TNSP of revenue from the sale of electricity on the *spot market* (negative) resulting from the *security service* asset being *enabled* at minimum *dispatch* or auxiliary *load* (if applicable).
FCAS	Frequency control *ancillary service/s*
IBR	Inverter based resource/s
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
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. For example, the minimum dispatch for a *generating unit* would be its minimum stable *generation* level required to provide the *system security service*.
Non-energy costs	FCAS payments, participant fees and other fees; if or where relevant.
NOS	Network outage scheduler
NSCAS	*network support and control ancillary service/s* Services with the capability to control the *active* or *reactive power* flow into or out of a *transmission network* and that either: a) act to maintain the *security* and supply r*eliability* of the *transmission network* in accordance with the *power system security standards* and the *reliability standard*. These are referred to as 'Reliability and security ancillary services' (RSAS). b) maintain or increase the capability of the *transmission network* to maximise net economic benefits to all those who produce, consume, or transport electricity in the market. These are referred to as 'Market benefits ancillary services' (MBAS).
Provider	A *System Security Service Provider* who is providing *system security services*, or a party *w*ho has agreed with a *System Security Service Provider* to provide *system security services*, as appropriate.
Procedures	*Security Enablement Procedures*
Schedule	A schedule issued by AEMO identifying the *system security services* AEMO intends to *enable* during the period covered by the schedule.
Security Enablement Procedures	The procedures to be made by AEMO in accordance with NER 11.168.2(a), which will replace these Provisional Procedures by operation of NER 11.168.2(d).
Security service asset	A *production unit, network element,* other *plant* or *facility* that is under an agreement to provide a *system security service*/s.
Spot market operation	A *security service* asset is in *spot market* operation if it is operating for the purpose of earning *energy* revenue and/or FCAS revenue.
Security service	A *system security service*
System security service	A *system security service* as defined in the NER, being: a) a *system strength service*; b) an *inertia network service;* c) *a NSCAS*; or d) a *transitional service*, to the extent procured by AEMO or a TNSP under an agreement for that service under the NER.
Threshold cost saving	The amount of forecast cost saving that must be exceeded in a forecast before a new schedule is adopted and update enablement instructions are issued. This will be a $ value set by AEMO in discussion with industry.
transitional services	A service provided by *plant*, equipment or *facilities* to meet a *power system security* need as a result of the transition to a low- or zero-emissions *power system*
TNSP	*Transmission Network Service Provider*
Usage payment	A payment to compensate the Provider for costs of operating in the manner required to provide the relevant *system security service.*

1.1.2. Interpretation

The following principles of interpretation apply to these Procedures unless otherwise expressly indicated:

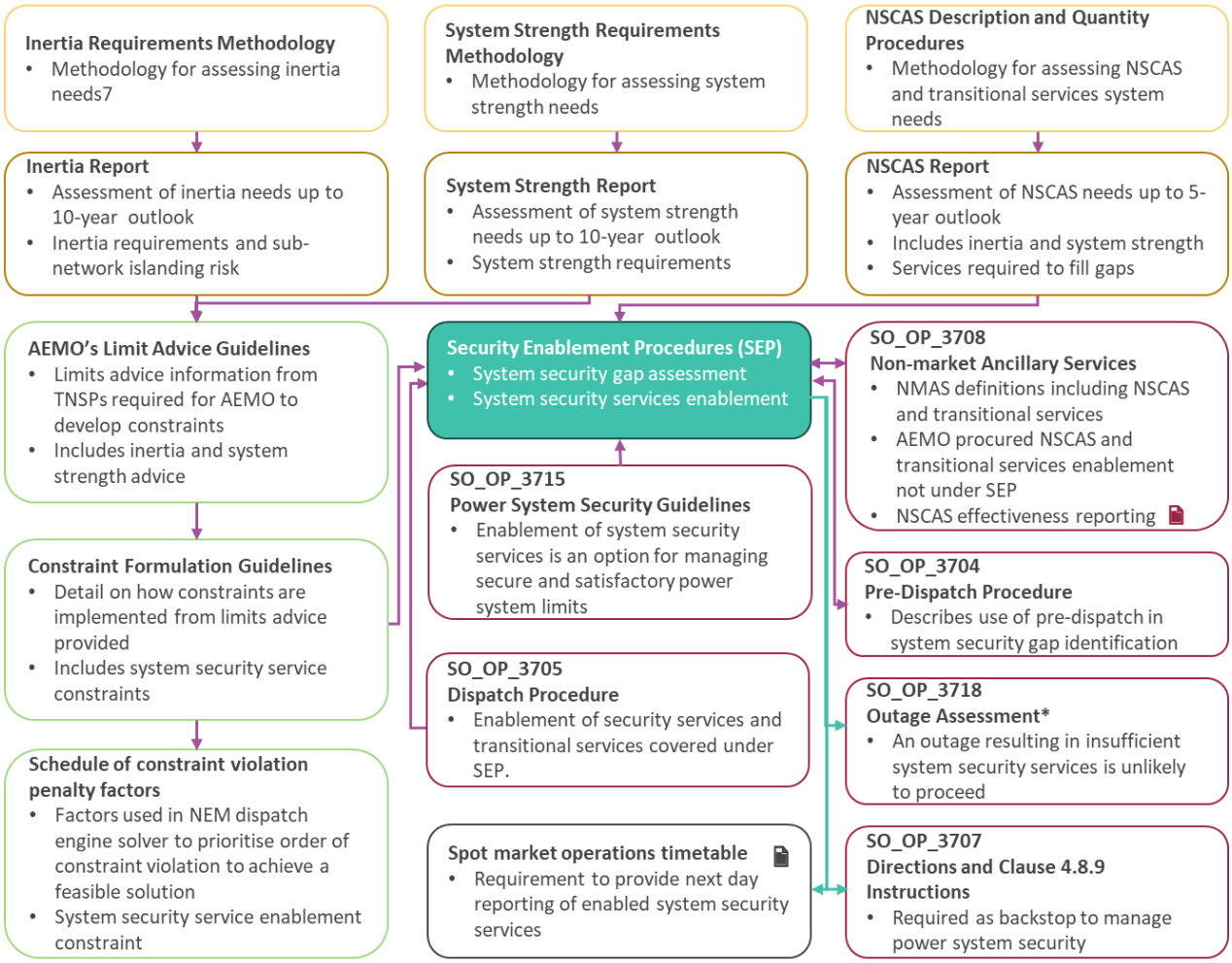
(a) These Procedures are subject to the principles of interpretation set out in Schedule 2 of the National Electricity Law.

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

1.1.3. Relationship of Procedures to other procedures and guides.

Figure 1 is a representation of how other key procedures and guides relate to these Procedures and their interdependencies.

Figure 1 Relationship between Security Enablement Procedures and other key operational documents



***SO_OP_3718 Outage Assessment**
System security services help AEMO manage secure and satisfactory operating conditions. Additional constraint sets may be invoked for outage conditions in accordance with NSP limits advice. Planned outages that impact availability of system security services may not be given permission to proceed (taking into consideration overall availability of scheduled resources).

2. Minimum System Security Requirements

Section 2 discusses the determination of the *minimum system security requirements*.

Under NER 4.4A.6(a)(1) AEMO must develop '*a methodology for how AEMO will determine the minimum system security requirements in accordance with clause 4.4A.3*'. NER 4.4A.3 states:

> *'(a) AEMO must, from time to time, publish, in accordance with the Security Enablement Procedures, the minimum system security requirements.*
>
> *(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: ….'*

The *minimum system security requirements* are those necessary for AEMO to operate the *power system* in a *secure operating state*[1] and to allow AEMO to meet the general principles for maintaining *power system security*[2] during the range of actual operating conditions encountered in the power system. Accordingly, AEMO should operate the *power system* in a *secure operating state* and be able to always return the *power system* to a *secure operating state* as soon as practicable, and at most, within 30 minutes of a *contingency event.*

AEMO will determine the *minimum system security requirements* through operational implementation of the requirements identified in the following documents:

- the annual Inertia Report[3], prepared in accordance with the Inertia Requirements Methodology[4],made under NER 5.20.4.
- the annual System Strength Report[5], prepared in accordance with the System Strength Requirements Methodology[6] made under NER 5.20.6.
- the annual NSCAS Report[7], prepared in accordance with the NSCAS Description and Quantity procedures[8], made under NER 5.20.2.
- the statement of security needs for *transitional services* (as defined under NER 3.11.11 (b)) published in accordance with the Transitional Services Guideline[9].

Table 1 specifies the *minimum system security requirements* and how they will be implemented in operational timeframes.

---

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

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

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

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

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

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

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

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

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

Table 1 Implementing minimum system security requirements in the operational timeframe

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[10]. For the mainland regions, these will be adapted for use in operational timeframe through the implementation of *security service 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. For Tasmania, AEMO and TasNetworks monitor inertia levels in real time through use of an operational tool. AEMO may enable a TasNetwork's contracted service to maintain sufficient levels, often through consultation with TasNetworks.
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* [11].	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[12]. TNSP's (*system strength service providers*) are required to use all reasonable endeavours to procure sufficient assets and services to ensure that these planning requirements can be met continuously. For the mainland regions 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 must provide AEMO with specific limits advice in accordance with AEMO's Limits Advice Guidelines[13] to inform the development of these *constraints* and to ensure consistency with the modelling and assumptions used by TNSPs in selecting their suite of *system strength service Providers*. For Tasmania, AEMO and TasNetworks monitor system strength in real time through use of an operational tool. AEMO may *enable* a TasNetwork's contracted service to maintain sufficient levels, often through consultation with TasNetworks.

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

[11] 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.

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

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

Service	Component	How requirement will be implemented in the operational timeframe
NSCAS	An identified *NSCAS gap* that AEMO considers must be remediated to maintain the *power system* in a *secure operating state.*	Requirements will be calculated consistent with the nature, timing, and magnitude of the corresponding *NSCAS gap*, as declared in AEMO's annual NSCAS Report[14]. 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.

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

3. System Security Services Enablement

Section 3 discusses the *enablement* methodology to meet *minimum system security requirements*.

Under NER 4.4A.6(a)(2) AEMO must develop '*a methodology for the enablement of system security services in accordance with the enablement principles in clause 4.4A.4*'. The *enablement* principles under NER 4.4A.4 are:

> *'(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*.'

The methodology for *system security services enablement* will align with the following *enablement* processes in Table 2. The methodology for achieving the *stable voltage waveform requirements* is discussed in Section 5.

Table 2 Enablement Processes

Requirements	Service	Proposed Enablement Process
Minimum system security requirements	*Inertia*	Automated *system security services enablement* (see section 3.1) or fallback to manual *system security services enablement* as required (see section 3.3).
	System Strength	
	NSCAS	Manual *system security services enablement* (see section 3.2) or automated in the *security service* scheduler if service definition and contract structure permits or automated via alternative AEMO system.
	Transitional	
	Other	
Stable voltage waveform requirements	*System Strength*	Enablement for the *stable voltage waveform requirement* (see section 5).

3.1. Automated system security services enablement

The automated *system security services enablement* process will be used to schedule *inertia* and *system strength services* to meet the *minimum system security requirements*.

The required steps for the automated process are illustrated in Figure 2 and described in further detail in Table 3.

Figure 2 High Level System Security Enablement Process

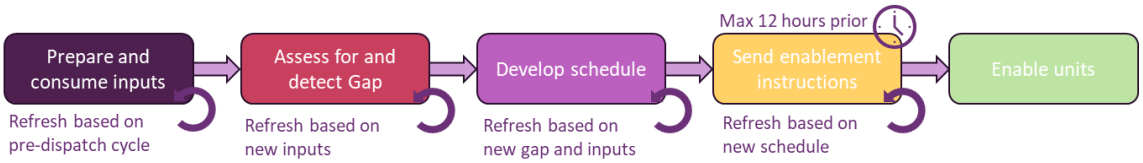


Table 3 Automated enablement process steps

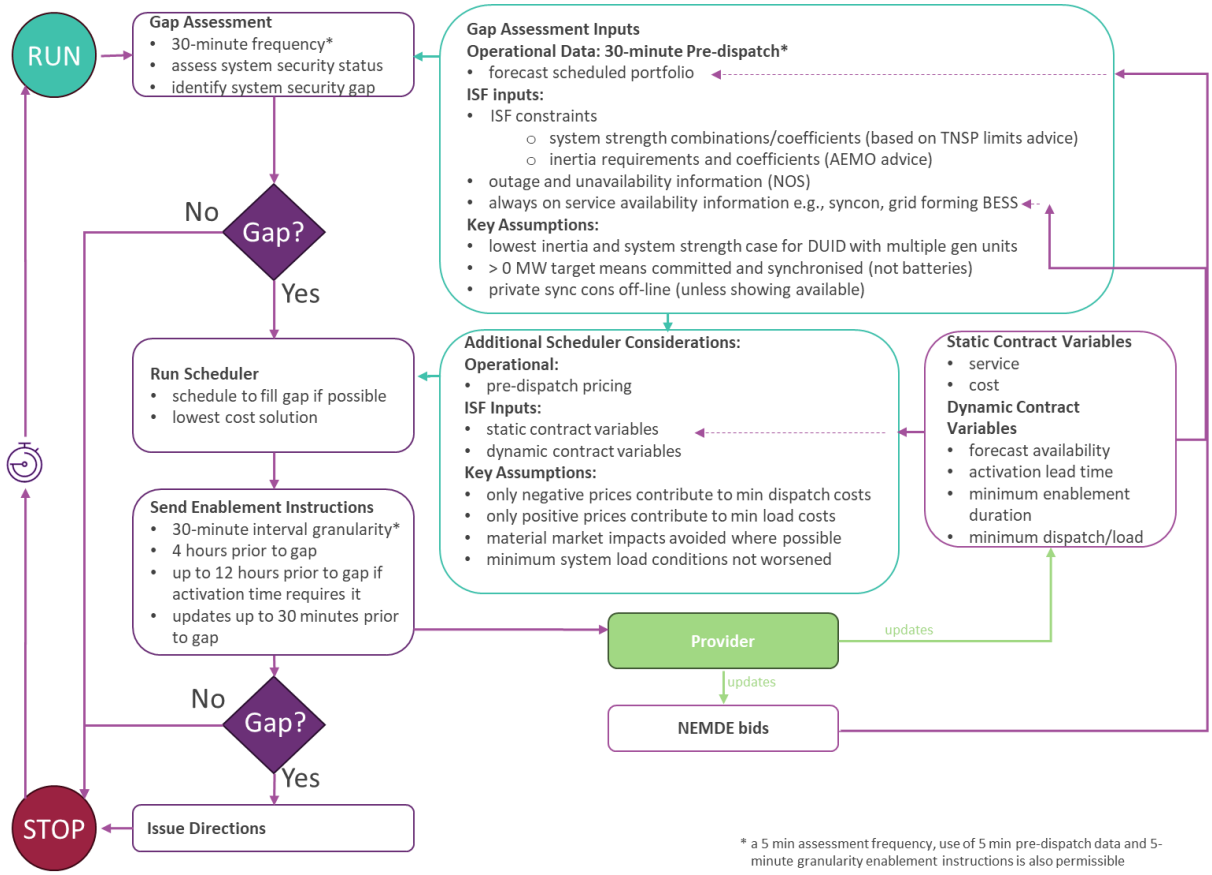
System Security Enablement Step	Detail

Prepare and consume inputs	• Establish *minimum system security requirement* in accordance with methodology
	• Source inputs from:
	  ○ TNSP limits and AEMO advice for *system strength* and *inertia*
	  ○ *pre-dispatch* to forecast portfolio of resources online
	  ○ network outage scheduler (NOS) to understand line outages, synchronous condenser *status and other relevant equipment status*
	  ○ *Provider interface for Providers' security service assets' availability*

Assess for and detect Gap	• Determine level of *system strength* and *inertia* that is forecast to be online prior to any *security service enablement* • For each *pre-dispatch* period compare *minimum system security requirement* with *system strength* and *inertia* forecast • If *system strength* or *inertia* is not forecast to meet *minimum requirement* identify a shortfall/gap
Develop Schedule	• Retrieve availability, *security service* details (activation lead time, service volume, minimum enablement duration) and cost of services that can meet identified gap • Establish a least cost solution for the *pre-dispatch* timeframe • Rerun process as new data becomes available and forecasts are updated
Send Enablement Instructions	• Send *enablement* instructions to Providers with activation lead times greater than IEI hours at the activation lead time before the identified gap • Send *enablement* instructions to Providers with activation lead times of IEI hours or less IEI hours before the identified gap. • Where a gap is identified within IEI hours send *enablement* instruction as soon as practicable. • Amend (update, cancel) instructions to Providers based on latest schedule as soon as practicable
Enable units	• Providers must comply with enablement instructions and • Providers must update dispatch bids as required to reflect *enablement* • Providers with a minimum enablement duration must bid to reflect that run time

The operational flowchart in Figure 3 provides context to how AEMO's *enablement* process will consume data and the types of data that may be included.

Figure 3 Potential Assumptions and Inputs in the Enablement Process



3.2. Manual system security services enablement

System security services that cannot be scheduled through the automated *enablement* system will be managed outside the automated process described in Section 3.1.

The key steps for a manual process are identified below and illustrated in Figure 4:

1. Definition of the threshold to trigger service enablement.

   For *NSCAS* this will be the identified *NSCAS gap* that has been procured by AEMO as provider of last resort or procured by the TNSP through a service which AEMO has agreed to enable.

   For transitional services this will be the level published in a statement of need.

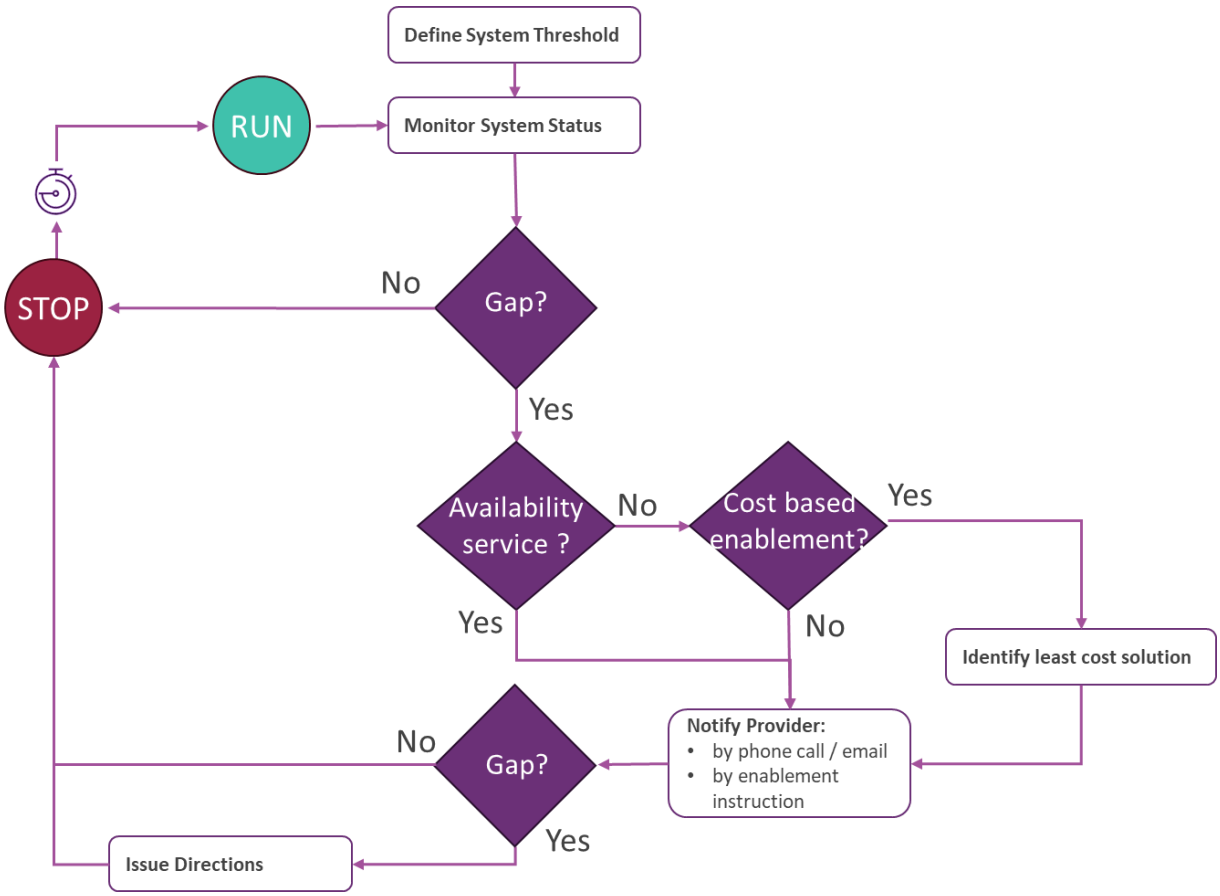
2. Monitor the system conditions to identify if the threshold level is forecast to not be, or currently not being, met, i.e., there is a *security service* gap identified in the forecast operational conditions.

3. Notify Providers that are on availability (on-going service provision) contracts of potential gap in the manner specified in Section 3.5.

4. *Enable* contracts based on pre-established priority list that takes account of service, activation timing and cost.

5. *Enable* service(s) in accordance with NER 4.4A.5(b) and cease *enablement* instruction in accordance with NER 4.4A.5(c) in the manner specified in Section 3.5.

Figure 4 Steps in Manual Enablement Process



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' will apply.

3.2.1. Manual system security enablement in Tasmania

In Tasmania, AEMO will manually provide an electronic signal to enable a *system security service* following identification of a gap and agreement with TasNetworks (if required) that enablement is required to meet *minimum system security requirements*. AEMO considers that this is the most effective way for the Tasmanian region to meet the *enablement principles* described in section 3.4.

3.3. Fallback enablement mechanism

Where necessary to do so AEMO will run manual processes that prioritise *maintaining power system security*. AEMO will:

- Inform the market via a market notice of suspension of the automatic *enablement* process (if required)
- Implement any combination of the following:
  - Cancel erroneous *enablement* instructions
  - Amend scheduler inputs and schedule ad-hoc runs
  - Adopt a manual *enablement* process

- Issue directions or instructions under NER 4.8.9.

This fall back mechanism will be implemented as required to ensure *power system security*, examples of where AEMO will consider the fallback enablement mechanism include situations where the automatic *enablement* process:

- fails to provide a solution that addresses the *security services* gap
- does not allow AEMO to return the *power system* to a *secure operating state* within 30 minutes of a *contingency event*
- *enables security service* assets which result in *security* issues in *pre-dispatch*, for example, a network limitation
- is not available or fails to run.

Implementation of the fallback mechanism will prioritise *power system security*. It will only take the enablement principles into account where practical to do so.

3.4. Enablement principles

AEMO will use reasonable endeavours to give effect to the *enablement* principles in NER 4.4A.4.

3.4.1. Lowest system security service cost

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

AEMO will determine the lowest cost *system security services* schedule for enablement through assessment of:

- The availability of *security service* assets to provide a service.
- The timing of the forecast gap.
- The activation lead times of available *security service* assets.
- The minimum *dispatch* levels.
- The level of *inertia* or *system strength* available from each *security services* asset.
- The financial parameters (payment types and values)
  - Activation payments ($ per activation)
  - Usage payments ($ per hour of enablement)
  - Energy revenue (minimum dispatch MWh x min[0, pre-dispatch price] $/MWh[15])
- Operational factors, for example, avoidance of minimum system *load* conditions.

Further details on the technical and financial parameters taken into account are set out in section 4.2.1 and section 4.3.

[15] In the case of Auxiliary Load related Energy Revenue payments, this calculation is adjusted to minimum dispatch MWh x max[0, pre-dispatch price] $/MWh

3.4.2. 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 *system security service enablement* processes conducted by *AEMO* will establish guardrails of the following operational requirements:

- *Providers* will be sent *enablement* instructions at the activation lead time or IEI ahead of the identified need, whichever is sooner.
- No *system security services* will be enabled greater than 12 hours in advance of the start of an identified need.
- *Providers* can be sent updated *enablement* instructions up to 5 minutes in advance to cancel, update or amend an *enablement* instruction.
- If a lower cost schedule is identified, *AEMO* will only amend *enablement instructions* where the threshold cost saving is forecast to be achieved.

3.4.3. Minimum system security service intervention

The *enablement* principle under NER 4.4A.4(c) requires AEMO to use reasonable endeavours to *enable system security services* only when, in AEMO's reasonable opinion, the *minimum system security requirements* or *stable voltage waveform requirements* would not be otherwise met.

AEMO will use reasonable endeavours to only *enable system security services* when a gap in the *minimum system security requirements* or *stable voltage waveform requirements* is identified. AEMO will make the assumptions in Table 4 when determining whether a gap in the *minimum system security requirements* is anticipated.

Table 4 Key assumptions in determining a system security services gap

Issue	Assumption
DUID with multiple generating units Where a DUID has multiple units and a combination of these can be used to make the *dispatch* target then it is not possible to determine which combination is online. This means that the level of *inertia* and *system strength* provided by the DUID is not known.	• AEMO will assume the worst case scenario i.e., assuming that the combination of units with the least *inertia / system strength* provision is going to be online to meet the relevant *dispatch* target.
Grid forming batteries AEMO is not able to confirm whether a grid forming battery is in grid forming mode or guarantee the amount of service a grid forming battery will provide.	• Grid forming batteries that are Providers will be assumed to be in grid forming mode when they indicate their availability through the Provider interface. This is expected to be 100% of the time they are online. • AEMO will assume zero service provision from any grid forming batteries which are not Providers or have indicated they are unavailable through the Provider interface.
Synchronous Condensers It is not possible to know if private synchronous condensers are in service from *pre-dispatch* data**.**	• If the synchronous condenser is a Provider, the synchronous condenser operator will provide availability and status information through AEMO's Provider interface. • Where the synchronous condenser is not a Provider, AEMO will assume the worst case scenario (that it is offline), unless it is captured by a TNSP in the NOS, in which case AEMO will assume it remains available when not advised otherwise through the NOS itself.

Issue	Assumption
Spot market operation and enablement A *security service* asset that requires a minimum *dispatch* target to be *enabled* will be compensated in its contract for any energy costs (energy revenue, see Section 4.3). If that *security service* asset decides to operate above its minimum *dispatch* target, it is moving into commercial operation in favour of *system security service enablement* so *system security service* payments will cease. However, the *security service* asset will continue to provide the level of *enabled inertia* or *system strength* regardless of that decision. The minimum total cost requirement means it is no longer appropriate to continue to pay for the service. (See Section 3.4.5)	• An asset that moves from *system service enablement* to commercial operation will continue to be *enabled* but cease to be paid and must continue to provide the service until the *enablement* end time in the *enablement* instruction. • This assumption does not apply to *security service* assets, such as a battery, which can provide a service without *dispatching* or *consuming* energy as a byproduct of *enablement*

3.4.4. Variable operational parameters required to be restated

The Provider must, in the form required by AEMO's systems established for the purpose of automating *system security service enablement* and ingesting Provider information, provide:

- The current availability and a continuous forecast of availability to AEMO and the TNSP for the short term PASA timeframe and must immediately update AEMO and the TNSP if there is any change in current or forecast availability of the *security service* asset.
- The current activation lead time and must immediately update AEMO and the TNSP if there is any change in current activation lead time.
- The current minimum *dispatch* and must immediately update AEMO and the TNSP if there is any change in current minimum *dispatch*.

For further information on operational parameters see section 4.2.1

AEMO, in performing its scheduling and *enablement* functions, will not explicitly take into account any special timing requirements or other circumstances relating to when the *system security service* is expected to be available (other than those detailed in this section), nor any limitations to continuous service provision. Examples include availability during specific months only or during business hours only. If agreements include such special timing requirements or other circumstances, it will be the responsibility of the Provider to reflect these requirements via notification to AEMO of the availability of the *security services* asset in real-time in accordance with this section.

3.4.5. Spot market operation and enablement

This section applies to *security service* assets that are capable of and classified for *spot market* operation.

NER 4.4A.4(c) states: '*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;*'

A *security service* asset with a requirement for energy dispatch (such as a minimum dispatch) when *enabled* cannot undertake *spot market* operation concurrently with *enablement*. To ensure no *enablement* for provision of a *security service* that would be provided as a result of the *security service* asset's normal *spot market* operation, i.e, commercial dispatch:

- AEMO will cease any payment for an *enablement* instruction of any *security service* asset that operates above the current stated minimum *dispatch* level.

- The *security service* asset must provide the *system security service* throughout the *enablement* period as initially stated in AEMO's instruction for *enablement*, via *spot market* operation or by returning to *security service* enablement i.e. return to minimum *dispatch* level (so as not to create a *security* gap, nor with the intention of decommitting from operation prior to the end of the enablement period).
- A *security service* asset that moves into *spot market* operation during an *enablement* period and subsequently returns to minimum *dispatch* during that *enablement* period will be paid the *enablement payments* for the total time that it is at minimum *dispatch* during the *enablement* period.

A *security service* asset that does not have a requirement for energy *dispatch* when *enabled*, can undertake *spot market* operation as part of the *enablement* of *system security services*. The *security service* asset must continue to provide the *system security service* for the *enablement* period.

3.5. Form of System Security Enablement Instructions

In accordance with NER 4.4A.5(b), AEMO may at any time give an *enablement* instruction to a Provider stating that AEMO requires *system security services* to be *enabled*. To facilitate the giving of *enablement* instructions:

- AEMO will use all reasonable endeavours to issue a schedule indicating an intention to *enable* a *security service* asset at any time the *security service* asset is notified as available, allowing for the activation lead time. If AEMO has issued a schedule, AEMO may cancel or amend the schedule at any time.
- A schedule may be made for a time prior to both the intended period of *enablement* and the activation period.
- A *security* services asset may be selected for *enablement* by AEMO at or before the activation lead time.
- *Enablement* instructions will be given by AEMO in the manner specified in Section 3.5.1.

Instructions will be provided in 30 minute granularity initially but may be introduced in 5 minute granularity in the future.

In accordance with NER 4.4A.5(c) AEMO may at any time give an instruction stating that AEMO requires the provision of *system security services* to cease.

There is no minimum or maximum period for which services can be *enabled*, subject to the notified availability, activation lead time and any minimum enablement duration included in the automated *enablement* process.

3.5.1. Form and content of security services enablement instructions

For the automatic methodology:

Security service enablement instructions will be issued electronically via the AEMO Electricity Market Management System (EMMS) interfaces. (*Security service enablement* instructions will be issued separately from any *dispatch instruction.*)

A *security service enablement* instruction to provide a *security service* includes:

- *security service* asset identifier e.g., DUID or unit identifier (if relevant)
- *security service* type
- *security service* start time

- expected *security service* end time
- number of units to be *enabled* (where relevant)

An enablement instruction to amend a *security service* includes:

- security service amendment type

A *security service enablement* instruction may also include a mode of operation and a unit combination once this functionality is included in the automatic enablement process.

Amendment of an *enablement* instruction, i.e. update or cancellation, typically involves the change of the start time or the end time from the initial instruction or any subsequent update. It may also include a change in technical parameters, e.g. number of units *enabled* or other relevant technical attribute.

For the manual methodology:

Security service enablement instructions may be issued in the following forms

- as defined in the Provider's *security service ancillary services agreement* or agreed between AEMO and TNSP which may include the form of verbal, participant email and market notices
- electronically via the AEMO EMMS interfaces (triggered following manual input of instruction details).

3.5.2. Compliance with enablement instructions

A Provider of *system strength services* or *inertia services* must comply with an *enablement* instruction for *system security services* given under these Procedures in accordance with NER 4.4A.5.

Other Providers (*NSCAS* and *transitional services*) must comply with an *enablement* instruction given under arrangements approved by *AEMO* in accordance with NER 4.3.4(d)(4), 5.20B.6(e) or 5.20C.4(e) or as agreed with AEMO under an *ancillary services agreement*. For the avoidance of doubt these arrangements will require a Provider to comply with an *enablement* instruction given under these Procedures.

In complying with an *enablement* instruction, the following general service requirements must be met:

- The Provider must operate the *security services* asset in accordance with the NER and all applicable rules and procedures whilst providing the *enabled system security services*. This includes, but is not limited to, meeting its *Generator Performance Standards*, and *Primary Frequency Response* obligations.
- In accordance with NER 4.11.1(b), the Provider must ensure appropriate monitoring and control equipment is in place for the *security services* asset/s.
- When enabled to provide system security services, the Provider must comply with the instruction in a manner that is consistent with the form of operation required to provide the services in accordance with NER 4.4A.5(e)-(g) and these Procedures.
- Where the *security service* asset is scheduled *plant*, this includes submitting *bids* or *rebids* as soon as practical if a minimum *dispatch* level is required to provide a service, such that its *maximum available capacity* for *energy* is equal to its minimum *dispatch*. If necessary, AEMO will apply *constraint equations* in *central dispatch* to give effect to the *enablement instruction.*
- When instructed to cease providing *system security services*, the Provider must comply with the instruction in a manner that is consistent with the form of operation required to cease providing the services in accordance with NER 4.4A.5(e)-(g) and these Procedures.

- *Enablement* is consistent with the operational requirements in section 3.4.5.

4. TNSP System Security Services Agreements

Section 4 outlines the requirements for TNSP *system security services* agreements.

Under NER 4.4A.6(a)(3), AEMO must establish minimum or recommended requirements to be included in TNSP *system security services* agreements. These requirements cover the following aspects:

- General agreement structure.
- Defining service provision.
- Financial structure.
- Intended scheduling arrangements.
- General requirements.

Within each of these sections the minimum requirements or recommended requirements are outlined, as relevant.

4.1. General agreement structure

The minimum requirements with respect to the general structure of agreements, including requirements regarding the relationship between contractual terms and *security service* assets that are necessary to facilitate AEMO's approach to scheduling and *enabling system security services* are:

- Agreements must allow AEMO to individually *enable security service* assets.
- A *security service* asset must not encompass more than one DUID.
- A single agreement may cover multiple *security service* assets.

4.2. Defining service provision

4.2.1. Service parameters

The parameters set out in Table 5, Table 6 and Table 7 are minimum requirements to be defined within the agreement and must also be promptly notified to AEMO, including any agreed variations, in accordance with section 3.4.4 of these Procedures. Where an asset can operate in more than one mode and following implementation of a solution that takes mode of operation into account, these parameters must be provided for each mode.

The operational parameters in Table 5 and Table 6 and the financial parameters in Table 7 may be used by AEMO to determine the available services and the lowest cost schedule to meet the *minimum system security requirements.*

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).
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 – see Section 3.4.4.	• Defined in hours and minutes. Less than 5 minutes can be stated as zero. – Adjustable in real time for physical reasons – see Table 6. • 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 – see Table 6. • Will not have usage payment consequences. • Will have energy revenue transfer consequences that *AEMO* will take into account in scheduling and *enablement* as outlined in section 4.3.
Minimum enablement duration	• 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

The parameters in Table 6 are subject to change in the operational timeframe:

Table 6 Variable operational parameters

Category	Requirement	Description
Availability	• Current and forecast availability of the service across the full-time horizon covered by the information system. This is expected to change due to the physical condition of the security services asset.	• This is a binary available or non-available. – Spot market operation is considered available – Applies to units that provide a service in a DUID • It may be necessary to use availability reductions to manage operations around commercial conditions, such as the management of stored energy.
Activation lead time	• Details of any activation lead time. This may be restated from the default contractual parameters where physical conditions have changed.	• See Table 5 for detailed description • Must maintain consistency for units that provide a service in a DUID • An example is where a generator has recently been operating and can therefore achieve a shorter activation lead time.
Minimum dispatch	• Details of any minimum *dispatch*. This may be restated from the default contractual parameters where unusual physical conditions have arisen.	• See Table 5 for detailed description • Adjustment will have energy revenue consequences • Adjustment will not impact usage payments • An example is where poor fuel quality or ambient conditions has temporarily raised the minimum stable boiler flame and resulting generation.

It is a minimum requirement of agreements that the Provider must ensure the *security service* asset is at all times prepared to deliver *system security services* in a manner that is consistent with its availability, activation lead time and minimum dispatch. This includes ensuring that the Provider is able to procure fuel or replenish stored energy within the activation lead time. If it is unable to do this, the asset is considered unavailable and the Provider should immediately update AEMO and the TNSP of this change in availability.

In accordance with NER 4.4A.1(a) AEMO may *enable* any *security service* to achieve and maintain the *minimum system security requirement.* When utilising a *security service* for a requirement that it was not initially contracted for AEMO will ensure that the *security service* can efficiently meet the *system security* requirement. Where this is not the case directions or instructions under NER 4.8.9 will be used until services are procured to meet the relevant requirement.

4.2.2. General service provision requirements

It is a minimum requirement that agreements recognise, and do not contain provisions that are inconsistent with:

- the general service requirements for complying with an *enablement* instruction outlined in section 3.5.2; and
- the operational requirements in section 3.4.5.

4.2.3. Parameters AEMO will not consider for scheduling

It is recommended that the below parameters are not included in agreements and that TNSPs seek to manage operational constraints within the fixed and variable parameters described in section 3.4.1. To confirm, for consistent scheduling and *enablement*, AEMO will not take the following contractual terms into account:

- Minimum off time. It is recommended that the activation payment to be used to cover the cycling costs of any length of off time. In addition, Providers should manage minimum off time requirement by updating their availability.

- Maximum run time. AEMO will assume that *enablement* can continue without limitation. Any restriction on *enablement* timing should be managed through restatement of availability.
- Real-time stored energy requirements. Where stored energy must be retained to provide service, this is the responsibility of the Provider, not AEMO scheduling. On occasion this may result in a change to, and require restatement of, availability and activation lead time.
- Ramp rates.

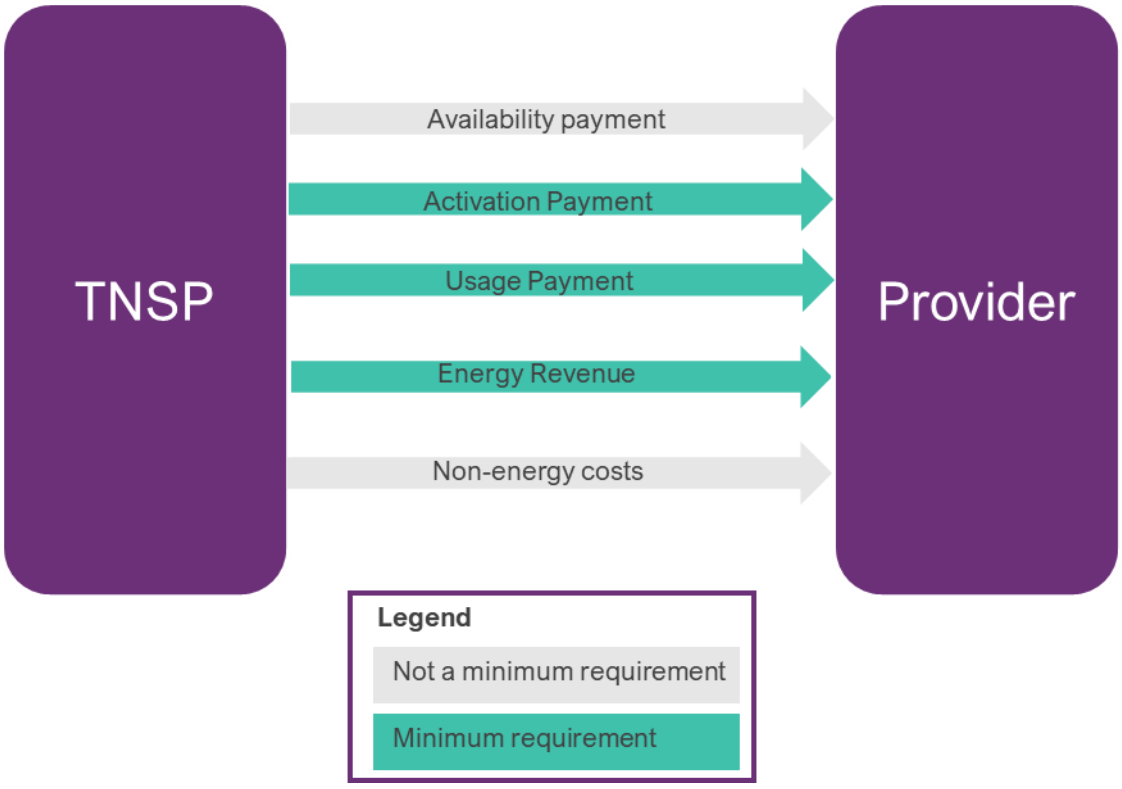
4.3. Financial structure

This section sets out minimum requirements with respect to the financial structure of agreements.

AEMO will not be a party to agreements between TNSPs and Providers but will be responsible for day to day *enablement* of services provided under those agreements. Accordingly, AEMO will not be liable for any costs or liabilities that arise when the agreement is in operation, including any unanticipated costs that are not adequately provided for in usage payments and activation payments. Similarly, AEMO will not play a role in settling these agreements; all settlements are between the TNSP and Provider. Any *spot market* settlements between *AEMO* and the Provider are unaffected.

The following diagram provides an overview of AEMO's expectations in broad terms for the financial structure of agreements and indicates which payment flows are taken into account for the purpose of *enabling system security services.*

Figure 5 Financial structure



The broad forms of settlement that may be incorporated in agreements are:

- An availability payment, which is assumed to compensate the Provider's fixed costs for maintaining the availability of the *system security service*, including profit and performance incentives. AEMO will not take these payments into account in its daily scheduling and enabling activities.
- A usage payment ($/hr), which is to compensate the Provider for costs (if applicable) of operating in the manner required to provide the relevant *system security service*.
- An activation payment ($/activation), which is to compensate the Provider for the cost of commencing operation from a previously inactive state.
- Energy revenue ($), which is the transfer of energy revenue between the Provider and TNSP, from the sale of electricity on the spot market resulting from the *security service* asset being *enabled* at minimum dispatch (if applicable).
- Non-energy costs: any exchange of FCAS payments, participant fees and other fees; if or where relevant. These are to be considered as separate items to activation payments, usage payments and energy revenues.

It is not a minimum requirement that agreements make provision for availability payments or non-energy costs, as AEMO will not take these payments into account in its daily scheduling and enabling activities. These may or may not be included in agreements at the discretion of TNSPs and Providers.

It is a minimum requirement that:

- agreements make provision for usage payments, activation payments and energy revenue. This does not, however, require that they have non-zero values. The value of usage payments and activation payments may be specified as zero, and energy revenue may be specified as zero. In this manner, TNSPs and Providers have flexibility as to the value of the financial flows for each payment type required to be included in an agreement.
- these payments are stated separately to each other in agreements. This is necessary for AEMO to establish a consistent and workable scheduling function. For example, if a single payment type was prescribed in a contract that represents the intent of both energy revenue ($) and usage payments ($/hr) combined, this would not be workable for the purpose of AEMO's scheduling function.
- the payments in an agreement for an asset or unit(s) that provide both system strength and inertia volumes when online are identical. That is, the cost of *enabling* the *system security service* is not reflective of the service type. The payment types included in AEMO's scheduling function are detailed in Table 7. It is recommended that agreements recognise, and do not contain provisions that are inconsistent with, the activation and *enablement* arrangements set out in these Procedures.

If AEMO's system can take account of the minimum enablement duration of a unit in the determination of the lowest cost schedule, then it must do so. Otherwise, the TNSP must provide AEMO with an approximation of the cost of usage and energy revenue for the minimum enablement duration as part of the activation cost of the service.

Where TNSP's establish agreements that do not match the provisions in this Procedure it is a minimum requirement that they provide to AEMO an approximation of values that are consistent with the usage, activation and energy revenue payment categories arrangements to allow AEMO to approximate the value of *enablement* in the scheduling system.

Table 7 Financial parameters in AEMO's scheduling system

Category	Definition	Stipulations
Usage payment	The payment, stated on a per hour basis, that the Provider will receive from the TNSP when the service is *enabled*. Usage payments (if relevant) are payable when the *security service* asset is *enabled* to provide services and would not otherwise be operating for the purpose of earning energy revenue (via *spot market* operation). Must be consistent for units that provide a service in a DUID	• Dollars per hour of service operation. – That is, not dollars per megawatt hour (MWh). • Settlement will be calculated on a *trading interval* basis. • Fixed but may be restated annually. – Intra-year revisions allowable with endorsement of service procurer where triggered via a verifiable cause, such as a change in fuel costs. Limited to a maximum of 1 intra-year revision per 30 days. Notification of an intra-year revision is to be provided to AEMO at least 5 business days prior to application. • Usage payments are not payable during the activation lead time. • Usage payment will not be adjusted for unforeseen costs. This payment does not change in real-time, even if: – Fuel prices or stored energy costs vary; – Minimum *dispatch* is altered. • The Provider must not be paid usage payments nor transfer energy revenue if *enablement* is discontinued for any reason.
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 *system security service* to be *enabled*. If the *security service* asset was already operating prior to AEMO selecting the *system security service* to be *enabled*, no activation payment is made. Must be consistent for units that provide a service in a DUID	• Fixed payment in dollars. • Fixed but may be restated annually. – Intra-year revisions allowable with endorsement of procurer where triggered via a verifiable cause, such as a change in fuel costs. Limited to a maximum of 1 intra-year revision per 30 days. Notification of an intra-year revision is to be provided to AEMO at least 5 business days prior to application. • If AEMO instructs the Provider to cease providing services or cancels or amends a schedule indicating an intention to *enable* a service: – If the instruction is given or schedule is cancelled or amended before the activation period, no activation payment is payable. – If the instruction is given or schedule is cancelled or amended within the activation period, the full activation payment is payable.
Energy revenue	Energy revenue ($) is the transfer of revenue from the sale of electricity on the *spot market* (negative) from the TNSP or AEMO resulting from the Provider being e*nabled* at minimum *dispatch* or auxiliary *load* (if applicable).	• If energy revenue is non-zero in an agreement, AEMO will adopt (for scheduling purposes) its standardised calculation in its scheduling processes that seeks to represent this payment associated with the minimum *dispatch* (where relevant) or auxiliary *load* (e.g. that associated with a synchronous condenser) to the Provider. This standardised calculation is described in section 3.4.1 as part of AEMO's enablement methodology. • AEMO will not consider any other form of transfer in its scheduling process. • The Provider must not be paid usage payments nor energy revenue if *enablement* is discontinued for any reason.

4.4. General requirements

The general minimum requirements for agreements are:

- Notwithstanding NER 11.168.2(e), agreements must include a requirement that, if *AEMO* reasonably requires them to do so for the purpose of scheduling and *enablement*, the parties will consult with *AEMO* on any existing agreement misalignment and negotiate in good faith to make any variations to the agreement that are required to ensure it operates in a manner that is consistent with the new processes.
- AEMO may require information from time to time to satisfy its scheduling and *enablement* obligations under NER 4.4A.1. Agreements must include a general obligation for Providers and TNSPs to provide information requested by AEMO in accordance with these Procedures.

AEMO intends to introduce more automated scheduling processes over time which may affect the operability of existing agreements. In this circumstance AEMO will work with TNSPs to agree any necessary changes to the *enablement* arrangements, including use of the above general minimum requirements.

5. Stable Voltage Waveform Requirements

Section 5 is the *enablement* process for the *stable voltage waveform requirements*.

NER 4.4A.1(b) states AEMO may *enable* '*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 NER 4.4A.6(a)(4) the Procedures must include '*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*'.

The *enablement* of services to support *stable voltage waveform* requires an understanding of the performance and outcomes of the *minimum system security services enablement* methodology to ensure the *enablement* principles under NER 4.4A.4 are met:

> *'(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*.'

5.1. Enablement for the stable voltage waveform requirement

AEMO will determine the level of the stable voltage waveform requirements in accordance with those levels articulated in TNSP limits advice, unless AEMO determines otherwise.

The operational processes to achieve and maintain the *stable voltage waveform* once *minimum system security requirements* have been met are described in this section.

5.1.1. Enablement process

Should AEMO be notified by TNSPs that a *system strength service* should be considered for *enablement* to meet the stable voltage waveform requirement, AEMO will:

- Receive limits advice from the relevant TNSP that articulates which *system strength services* should be considered for *enablement*, and which IBR units' additional *dispatch* is supported by the *enablement* of such *system strength services*;
- Consider what bespoke or manual processes AEMO can reasonably establish to *enable* such *system strength services*, having regard to the *enablement* principles and AEMO's ability to operationally manage such an arrangement.
- Where possible and appropriate under the enablement principles, prioritise utilisation of continuous services (or 'always on') *system strength services.*

- Consider delegation of the *enablement* function to TNSPs to meet stable *voltage waveform requirements* where appropriate, efficient and readily separable from scheduling for the *minimum system security requirement*.

6. Enablement Delegation

NER 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. NER 3.11.3(b2), 5.20B.6(b2) and 5.20C.4(b2) recognise that AEMO may agree to a TNSP *enabling system strength services* or *inertia network services.*

AEMO may delegate matters in this Procedure to a TNSP if the following conditions are met:

- The relevant TNSP must demonstrate a process for defining minimum system security requirements.
- The relevant TNSP can demonstrate a process for enabling system security services under contracts to meet requirements at lowest cost.
- Assessment of relevant TNSP's contracts and *enablement* process demonstrates to AEMO's satisfaction that TNSP *enablement* will be no less efficient than AEMO *enablement*.
- 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. For example, 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*.

Version release history

Version	Effective Date	Summary of Changes
1.0	30 June 2024	First provisional version for publication.
1.1	31 August 2025	Draft for consultation
1.2	31 August 2025	Draft for consultation