Stakeholder forum – Security Enablement Procedures Consultation

Wednesday 25 June 2025

1. Welcome

Jen Marin, Principal Advisor Industry Enablement

We acknowledge the Traditional Custodians of the land, seas and waters across Australia. We honour the wisdom of Aboriginal and Torres Strait Islander Elders past and present and embrace future generations.

We acknowledge that, wherever we work, we do so on Aboriginal and Torres Strait Islander lands. We pay respect to the world's oldest continuing culture and First Nations peoples' deep and continuing connection to Country; and hope that our work can benefit both people and Country.

'Journey of unity: AEMO's Reconciliation Path' by Lani Balzan

AEMO Group is proud to have delivered its first Reconciliation Action Plan in May 2024. 'Journey of unity: AEMO's Reconciliation Path' was created by Wiradjuri artist Lani Balzan to visually narrate our ongoing journey towards reconciliation - a collaborative endeavour that honours First Nations cultures, fosters mutual understanding, and paves the way for a brighter, more inclusive future.

Read our RAP

Agenda

#	Time	Topic	Presenter
1	13:00 – 13:05	**Welcome**	Jen Marin
2	13:05 – 13:15	**Project update**	Carla Ziser
3	13:15 – 13.30	**Draft transition approach**	Rosie Elkins
4	13:30 – 14:35	**Security Enablement Procedures first round consultation overview** • Summary of submissions and changes made • Relationship with other documents • Minimum system security requirements • System security services enablement • Market information • Operational considerations • TNSP system security service agreements • Stable voltage waveform • Enablement delegation • Other matters	Ruth Guest
5	14:35 – 14:50	**Q&A**	Jen Marin
6	14:50 – 15:00	**Meeting Close**	Jen Marin

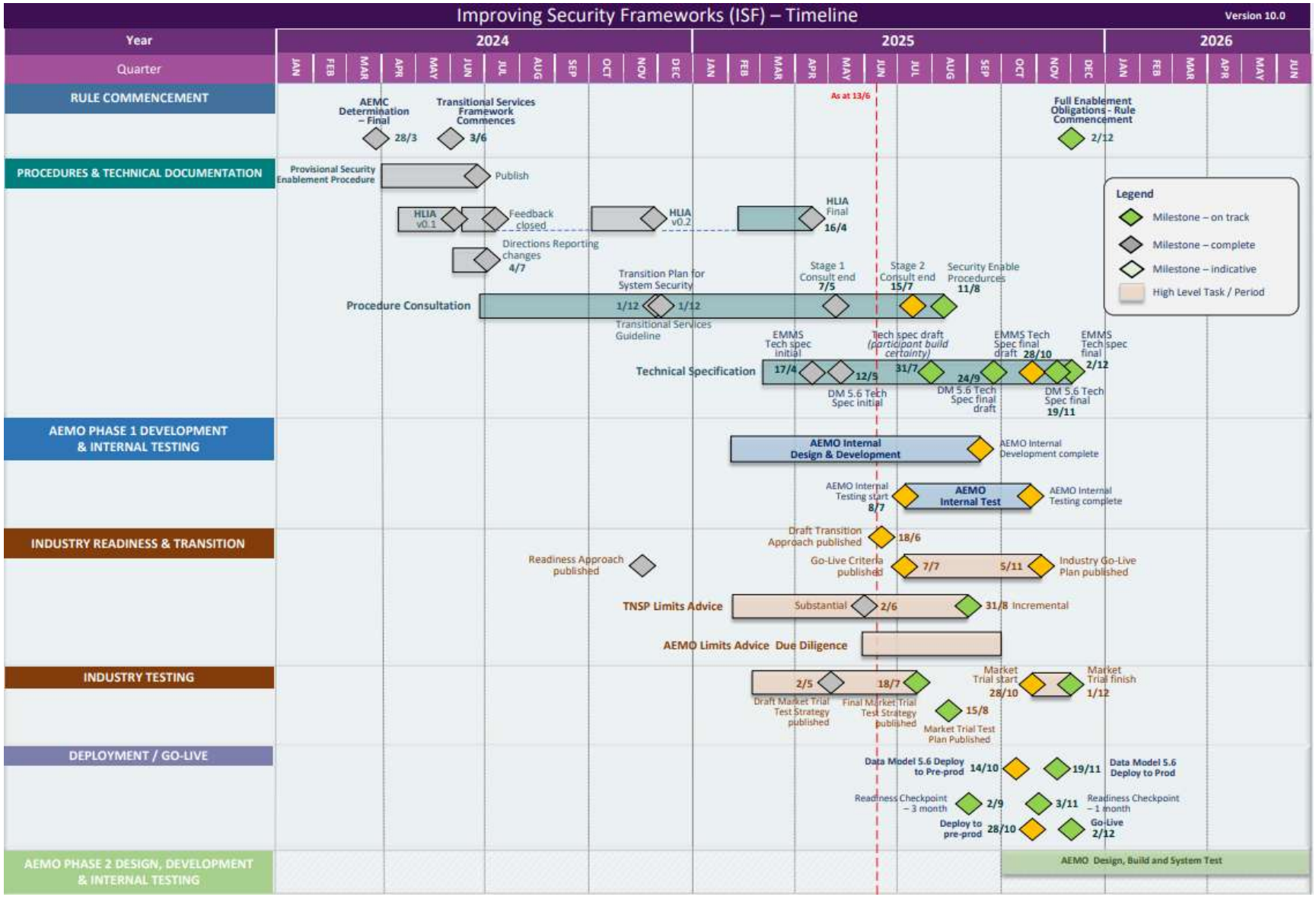
Appendix A: Competition law meeting protocol

"Please note that this meeting will be recorded by AEMO and may be accessed and used by AEMO for the purpose of compiling notetaking. By attending the meeting, you consent to AEMO recording the meeting and using the record for this purpose. No other recording of the meeting is permitted"

2. Project Update

Carla Ziser, Manager Wholesale Reform Delivery

Improving Security Frameworks Timeline



Progress Summary

Overall project status **AMBER**

- Identified dependencies for development of the scheduling system solution are at a high risk of impacting critical path.
- AEMO has revised the internal scope and delivery timeframes to mitigate the risks of compressed delivery timeframes, prioritising the delivery of scheduling system components for 2 December that Participants and TNSPs interface with, and ensuring business processes are in place (within AEMO) to manage a post-December delivery of remaining solution components. A compressed delivery timeline will remain.
- Several documents available to support industry preparation with more to come as initiative progresses
- **The AEMO-SSSP working group activities continue** alongside the project activities

ISF General Update

Revised delivery approach underway to manage enablement solution delivery risks

- To ensure AEMO is able to meet its rule obligations, and given considerable delivery complexity and compressed timeframes, AEMO has made changes to delivery timing of some solution components.
  - The revised delivery plan aims to minimise the impacts for participants by prioritising delivery of participant-facing components of the solution.
  - Fully automated scheduling functions (primarily internal to AEMO), and other non-core components of the solution will be delivered via subsequent releases and phases following the Rule commencement.
- AEMO is working to ensure required internal business processes are in place to support system security enablement functions from the go-live date of 2 December 2025.

Upcoming publications

- AEMO published a **Draft Transition Approach** on 17 June for comment to guide participants on AEMO's approach to transitioning to system security enablement. It is accompanied by a **revised draft Market Trial Strategy.**
- AEMO commenced the second-round consultation on the Security Enablement Procedure on 13 June.
  - Submissions are due on **15 July 2025.**

What's in and out of scope for Release 1?

In scope

Items remaining in scope prioritise components that Providers will interface with and support auditability of actions, including:

- External Portal, allowing Providers to input availability and variable contract parameters and access enablement instructions
- Internal Portal and post-processing functions that support the creation, amendment, cancellation and issuing of enablement instructions
- Automated creation of daily reports to fulfill Rule requirements, enablement information for TNSPs

Out of scope

Out-of-scope items to be delivered as part of Release 1.1 are as below and will become increasingly important as the number of available contracts and security actions increases:

- Solver and gap assessment functions
- Indicative rolling DUID schedules
- Credible contingency support functions
- Internal alerts & alarm management, and confirmation of enablement fulfillment
- Supervisory mode functions

- AEMO will have business processes in place to perform gap assessment, assess options & create enablement instructions
- AEMO's Transition Approach will address how agreements will be transitioned to the new enablement process (covered later in this session)

3. Draft Transition Approach

Rosie Elkins, Business Lead

Draft Transition Approach & Revised Draft Market Trial Strategy

The Draft Transition Approach reflects current system solution delivery plans that AEMO has in place to ensure it is able to meet its rule obligations, proactively manage transition risks, and support TNSPs and Providers to progressively transition to new system security enablement arrangements given considerable delivery complexity.

- AEMO has released a Draft Transition Approach as a high-level guide for TNSPs and Providers on:
  - Submission, assessment and obtaining approval of system security agreements
  - Demonstrating system preparedness, including via AEMO's Market Trial and extended support period
  - AEMO's process for transitioning from directions to enablement, noting expected timeframes and dependencies on solution readiness
  - Participation in accordance with the Security Enablement Procedure

- The Draft Transition Approach is accompanied by the publication of a **revised Draft Market Trial Strategy**. To better provide for a risk-managed approach to the introduction of new services enablement, AEMO has adjusted the Market Trial period to commence in late October, followed by an **extended transition support period for new security providers**.

Sep 2025	Oct 2025	Nov 2025	Dec 2025	Jan 2026	Feb 2026
	Initial Market Trial timeframe				
		New Market Trial timeframe	Extended transition support period		

Transition Approach – key milestones

Ongoing to 31 Aug 2025

Limits advice submission

TNSPs provide incremental updates to limits advice to AEMO

(substantive limits advice received by 31 May 2025)

Ongoing to 1 Sept 2025

TNSP contracting

Contracting in process (for both existing and new agreements)

Ideally contracts complete and submitted to AEMO by 1 Sept to facilitate inclusion in Market Trial

From 2 Sept 2025

Contracts Approval Process for TNSPs

Contracts Approval Process commences for submitted contracts as received

Stage 1 Contract Approval: conditional approval of contract

27 Oct 2025 to end Feb 2026

System preparedness - Market Trial & extended support period

TNSPs and Providers may participate in Market Trial as the first opportunity to demonstrate readiness in pre-production; to be followed with extended support period

Stage 2 Contract Approval: system readiness demonstrated & full approval

From 2 Dec 2025

Rule commencement

Rule commencement date for enablement of system security services contracts

AEMO will commence its transition to enablement processes, starting with manual enablement

From Feb 2026

AEMO will make agreements with TNSPs/ Providers for later contracts to progress through approval process and commence enablement

Contracts approval process

Contract & form submission

- Contract and approval request form submitted by TNSP to AEMO via email
- Includes submission of key contract parameters
- Assessment may occur in parallel with applicable AER approval process where relevant

Refer to:

Conditional contract approval & technical assessment

- AEMO will use best endeavours to review the contract to assess, within 20 business days:
  - Contract parameters are aligned with requirements in the NER & SEP
  - Technical specifications and performance standards and arrangements necessary to give instructions to enable or cease provision of the system security service.
- AEMO must provide the reasons for withholding approval and may advise the changes it requires to be made
- If approval is withheld, progression to conditional approval may only occur once additional information is received, and request is resubmitted

Refer to:

NER clause 5.20B.6 (relating to inertia services)

NER clause 5.20C.4 (relating to system strength services)

Demonstrate system preparedness

- Via pre-production environment – Market Trial, extended support period or BAU pre-prod testing process
- Participant verifies ability to interact with AEMO's systems, submit required information, receive enablement instructions, access reports etc

Refer to:

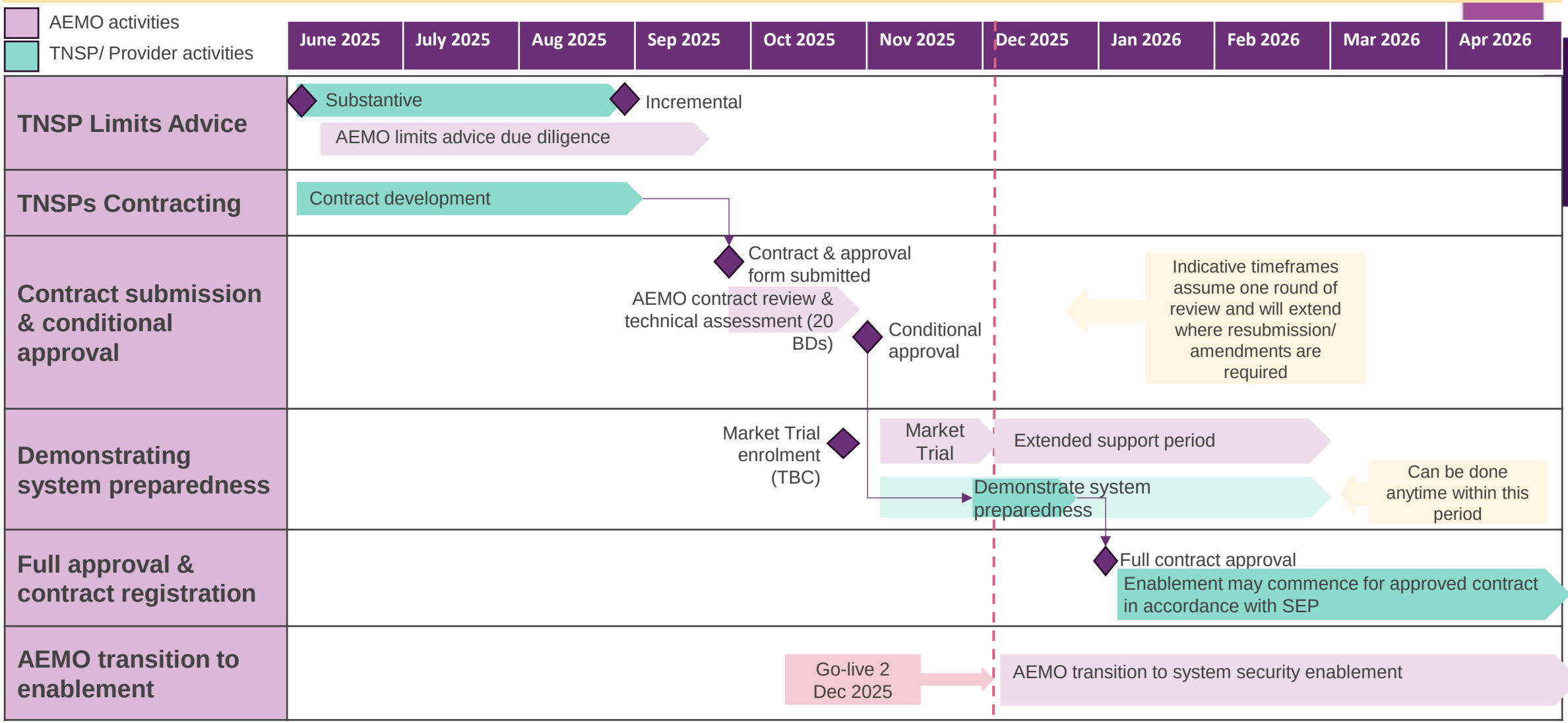
Full approval & Contract registration

- Once all steps are complete, AEMO will register the contract in its contract management system, the unit will be considered a system strength production unit or inertia production unit (as relevant) and enablement for system security services may commence in accordance with SEP

Refer to:

Consolidated transition approach

The example view below provides a summary of the **indicative** timeframes for transitioning a contract from submission to full approval, with system preparedness activities undertaken as part of the extended support period.



4. Security Enablement Procedures first round consultation overview

Ruth Guest

Summary of Submissions

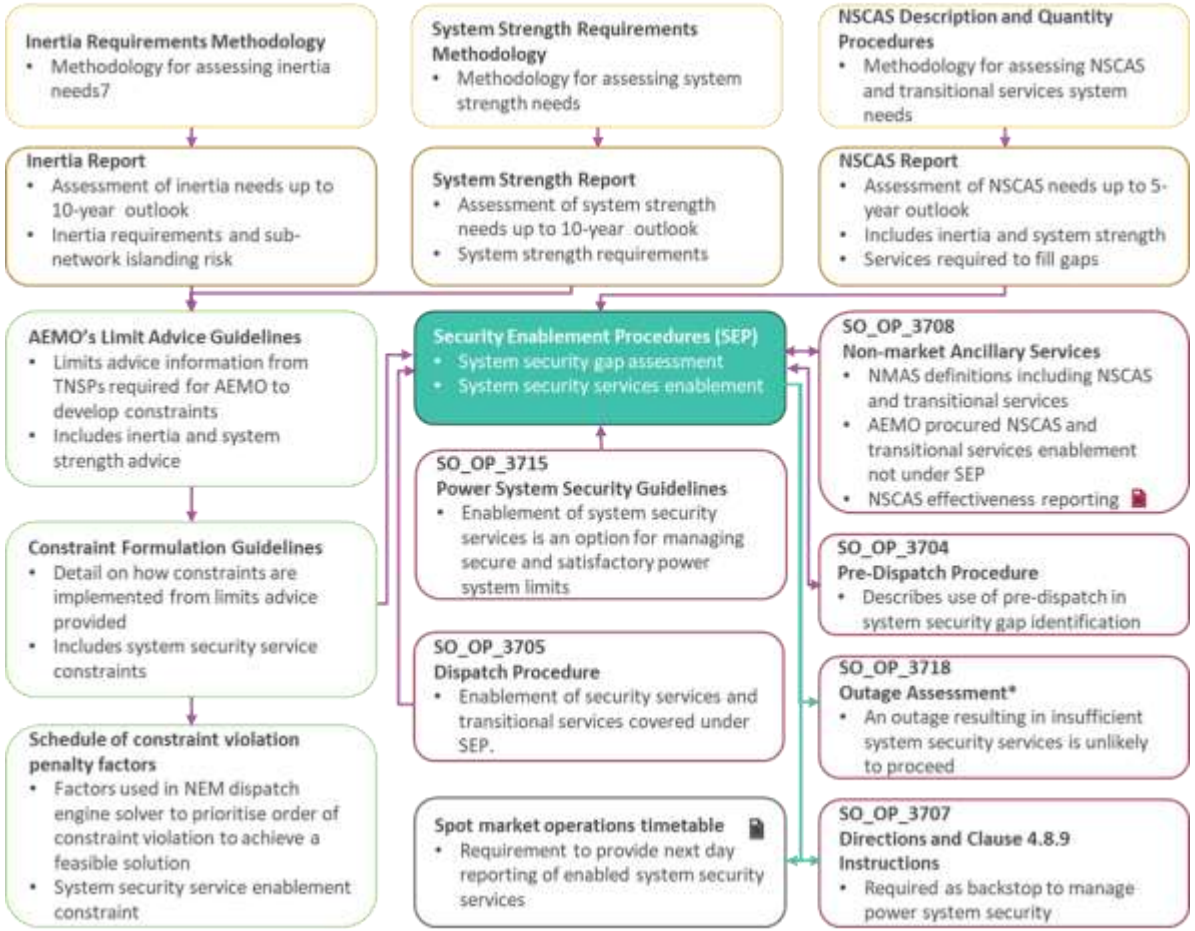
- AEMO thanks participants for their submissions and appreciates the well informed and comprehensive content included in the submissions
- 11 submissions were received in response to the first round of consultation of the Security Enablement Procedures (SEP), including 4 late submissions
- AEMO values a collaborative approach and has made changes to the SEP to reflect participants views
- The draft report addresses the following submission themes:
  - Minimum system security requirements
  - System security services enablement
  - Market information
  - Operational considerations
  - TNSP system security services agreements
  - Stable voltage waveform
  - Enablement delegation

Changes made to SEP to reflect stakeholder views

- Clarified the meaning of an *enablement instruction* and an *enablement instruction amendment*
- Included timing requirements for operational variables provision
- Clarified that TNSPs have a ‘reasonable endeavours’ obligation to meet system strength needs
- Added enablement to meet a system security gap should be consistent with the service contracted
- Clarified that stable voltage waveform should achieve ‘additional’ IBR dispatch
- Further amendments are covered in ‘other matters’

AEMO is also considering stakeholder comments in the context of the delivery approach, for example, market transparency, operational assumptions and annual reporting.

Security Enablement Procedures relationships with other documents



A new diagram has been added to provide context to the Security Enablement Procedures (SEP) and its relationship to documentation:

- called out in the SEP
- that guides activities referenced in the SEP e.g., directions
- with consequential changes because of SEP and/or ISF Rule.

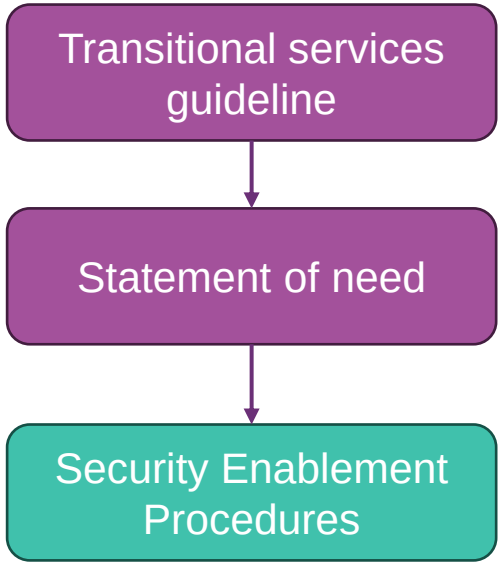
This will be updated in the final version to include :

- Transitional Services guideline
- Statement of Need

Minimum system security requirements

FEEDBACK

1. Broad discretion with no accountability for decisions
2. Set out detail for ‘other’ power system security requirements
3. How other power system security requirements would be communicated to market
4. Appreciate approach of allowing some flexibility in the procedure
5. Consistency underlying AEMO’s decision making supported



- NER 4.4A.3(b)(7) states *‘whatever is reasonably considered necessary by AEMO to maintain the power system in a secure operating state’* – this discretion was afforded to AEMO in the ISF Rule.
- ‘Other’ services, when identified and defined, will most likely be a transitional service subject to a published Statement of Need and procurement process. AEMO appreciates that stakeholders will want/need to be aware of what 'other' requirements might be if they arise and will make reasonable endeavours to be transparent at that time. It is not possible to provide further detail at this time – the intent in the SEP is to account for these unknown future services.

No change has been made to the SEP

System security services enablement

FEEDBACK

1. Should not differentiate enablement approach between technologies
2. Should not enable services for post contingency purposes
3. Clarify what an enablement instruction amendment means
4. Short lead time services should be catered for in scheduler
5. Unclear how an undefined service could be included in automated enablement
6. Improving automation overtime should be a focus

- The enablement approach is different between long and short lead technologies to cater for activation times, activation costs etc.
- AEMO considers paying for a service that is a by-product of commercial operation will not meet the lowest cost principle
- NER 4.2.6 requires AEMO to take reasonable actions to ensure it can bring the power system to a secure operating state within 30 mins following a contingency event. System security services will be required for this purpose.
- An undefined service will either fit into the automated enablement if constraints and payment structures allow, otherwise they will be manually enabled. The SEP affords this optionality, noting manually enablement is more likely
- AEMO intends to progressively improve the automated solution which should allow further stakeholder concerns to be progressively addressed

A change has been made to clarify the meaning of an enablement instruction and an enablement instruction amendment

Market information

FEEDBACK

1. Notify market of security services gap, enablement time and minimum time for service
2. Notification of system security gap via market notice mechanism
3. Communication to market on manual enablement activity
4. Details on operational decision making for a manual amendment

- AEMO recognises transparency is important and is intending to provide a pre-dispatch forecast view of system security service gap assessments to the market by region as part of a secondary phase of implementation
- To maintain flexibility, AEMO is not proposing to add an obligation for how market notification occurs in the SEP e.g., market notices.
- Assessment of the suitability of a given enablement instruction, or manual enablement of a service, is based on constraints that bind and a wide range of complex inter-related system outcomes. AEMO does not consider documenting further detail in the SEP is practical.
- The ‘day+1’ report required under NER 4.4A.7 will provide clarity on the enablement instructions that were issued to providers and their estimated cost
- For further transparency AEMO will provide information on the level of manual oversight as part of its annual report.

No change to Security Enablement Procedures

Operational considerations

FEEDBACK

1. Cancellation period should be longer to avoid market disruption
2. State the timeframe over which variable operational parameters should be restated
3. Assumptions for grid forming battery operation too conservative
4. Operators of private synchronous condensers should provide online status
5. Rationale behind 4-hour minimum enablement notice period
6. AEMO should adopt a more efficient assumption for multiple unit DUIDs

- AEMO is requiring providers to submit 7-day forecast availability information to allow an understanding of upcoming availability concerns for security services and outage management
- To meet the lowest cost principle AEMO believes that it needs to minimise cancellation times. Cancellation will only occur if gap reduces or a materially lower cost solution has been identified.
- An activation payment will be honoured if cancellation occurs within activation lead time
- An activation payment and minimum duration payment will be honoured if cancellation occurs within activation lead time or minimum duration time. AEMO believes this will provide service providers with the required outcomes to manage their operational and commercial risks.
- AEMO maintains the right to cancel at any time for power system security
- AEMO agrees that information on private synchronous condenser availability would be valuable, however AEMO has no power to require private synchronous condensers that are not service providers to provide this information
- AEMO has sought to balance certainty, visibility to market through pre-dispatch, and avoidance of instruction amendment by choosing the 4-hour notice period. AEMO is open to alternative views.
- AEMO agrees that unnecessary conservatism in assumptions is not efficient and will seek to improve assumptions with respect to multiple unit DUIDs and grid forming BESS over time

A change has been made to clarify the timing requirements for operational variables

TNSP system security services agreements

FEEDBACK

1. TNSP contract requirements by AEMO is an overreach
2. Requirements must be sufficiently clear and certain for TNSPs to meet ISF Rule obligations
3. AEMO must ensure that any enablement is consistent with the contracted service
4. AEMO to ensure contracts reflect least cost
5. TNSPs use reasonable endeavours to meet the system strength standard

- NER 4.4A.6(3) requires AEMO to establish minimum or recommended requirements of the system security services agreements to be entered into by TNSPs. Extensive consultation has been undertaken with TNSPs on this matter.
- AER has the obligation to ensure that the costs of a contracted service by TNSPs is appropriate
- AEMO agrees that a service that could meet an as-yet undefined need should only do so if this is an efficient outcome.

A change has been made to clarify that TNSPs have a ‘reasonable endeavours’ obligation to meet system strength needs and that enablement to meet a system security gap should be consistent with the service contracted.

Stable voltage waveform

FEEDBACK

1. Additional drafting to clarify when enablement for stable voltage waveform can occur
2. Appropriate for the period from 2 Dec 25 to 1 July 26

- AEMO has included the stable voltage waveform requirements definition under NER 4.4A.4(d) reproduced in the SEP
- AEMO is proposing to engage in detail with stakeholders on stable voltage waveform requirements later in the year to discuss when system security services should be used to increase IBR dispatch in accordance with the stable voltage waveform requirement. Updates to the SEP will be proposed and be the subject of a consultation process with stakeholders at that time.

A change has been made to clarify that stable voltage waveform should achieve ‘additional’ IBR dispatch

Enablement delegation

FEEDBACK

1. TNSP to calculate lowest market cost overall
2. Flexibility provided for is appropriate
3. Further work required prior to delegating

- AEMO considers that the conditions as written in the SEP will ensure that delegation only occurs if it is an efficient outcome for the market
- AEMO agrees that each delegation should be assessed on its merits at the time and take into account considerations such as transparency and least cost.
- AEMO notes that daily reporting will be required under NER 4.4A.7 regardless of any delegation.

No change to the Security Enablement Procedures

Other matters

- AEMO has included a diagram in the SEP to illustrate how other procedures, and importantly those with consequential changes, interact with the SEP.
- Updates have been made to allow for enablement during limited initial automation delivered on 2 December 2025 as well as in anticipation of delivery of a fully automated solution.
- The current process of gap analysis in Tasmania has been allowed for in Table 1 Implementing minimum system security requirements in the operational timeframe.
- Section 3.2.1 has been added to clarify the Tasmanian enablement process – considered the most efficient process for Tasmania
- AEMO intends to publish a factsheet on the Tasmanian gap assessment and enablement process for transparency in late June to allow participants to consider its contents in the context of the SEP consultation.
- The term ‘minimum run time’ is replaced with the term ‘minimum enablement duration’.

5. Q&A Session

Questions

5. Next Steps

Security Enablement Procedures Consultation Timelines

- **Consultation paper published**
  7 April 2025
- **Public forum**
  10 April 2025
- **Submissions due on consultation paper**
  8 May 2025
- **Draft report published**
  13 June 2025
- **Submissions due on draft report**
  15 July 2025
- **Final report and procedure published**
  Expected 11 August 2025

Submissions due 15 July 2025

https://aemo.com.au/consultations/current-and-closed-consultations/security-enablement-procedures

Close

NEMReform@aemo.com.au

Improving Security Frameworks for the Energy Transition

Appendix A:
Competition law meeting protocol

AEMO Competition Law - Meeting Protocol

AEMO is committed to complying with all applicable laws, including the Competition and Consumer Act 2010 (CCA). In any dealings with AEMO regarding proposed reforms or other initiatives, all participants agree to adhere to the CCA at all times and to comply with this Protocol. Participants must arrange for their representatives to be briefed on competition law risks and obligations.

Participants in AEMO discussions **must**:

- Ensure that discussions are limited to the matters contemplated by the agenda for the discussion
- Make independent and unilateral decisions about their commercial positions and approach in relation to the matters under discussion with AEMO
- Immediately and clearly raise an objection with AEMO or the Chair of the meeting if a matter is discussed that the participant is concerned may give rise to competition law risks or a breach of this Protocol

Participants in AEMO meetings **must not** discuss or agree on the following topics:

- Which customers they will supply or market to
- The price or other terms at which Participants will supply
- Bids or tenders, including the nature of a bid that a Participant intends to make or whether the Participant will participate in the bid
- Which suppliers Participants will acquire from (or the price or other terms on which they acquire goods or services)
- Refusing to supply a person or company access to any products, services or inputs they require

Under no circumstances must Participants share Competitively Sensitive Information. Competitively Sensitive Information means confidential information relating to a Participant which if disclosed to a competitor could affect its current or future commercial strategies, such as pricing information, customer terms and conditions, supply terms and conditions, sales, marketing or procurement strategies, product development, margins, costs, capacity or production planning.

AEMO

AUSTRALIAN ENERGY MARKET OPERATOR

For more information visit

aemo.com.au