SSM System Preparedness Testing – Fact Sheet

Fact Sheet

Introduction

This fact sheet is relevant to contracted System Security Service Providers who will submit their operational information to, and receive enablement information from, AEMO's Security Service Management (SSM) interface via the Markets Portal.

The intent is to provide System Security Service Providers with an overview of the Markets Portal functions that will be used during System Preparedness Testing. This will ensure participants are aware of what to expect, what actions they will need to complete, and confirm system readiness is established prior to commencement of enablement activities.

System preparedness testing can be undertaken as part of AEMO's Market Trial (commencing October 2025), or subsequently as part of AEMO's BAU System Preparedness Testing process (after November 2025).

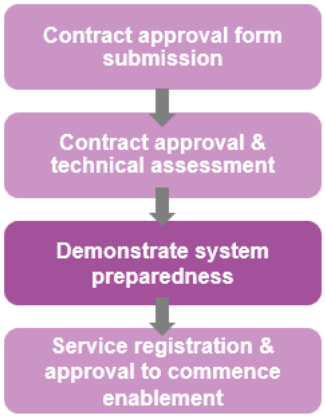

Figure 1: Contract approval and registration process

Please refer to the December 2025 EMMS Technical Specification for guidance on accessing and using the new SSM interface and the detailed technical requirements, including system changes to support ISF, API, and reporting.

SSM Portal Access

Participants will gain access to the SSM interface through the AEMO Markets Portal.

Existing Registered Participants

Existing Market Participants must ensure their existing Participant Administrator (PA) assigns the appropriate user access via the User Right Management tool. For a guide on how to do this, please refer to the AEMO Guide to User Rights.

In instances where the service provider is not the Financially Responsible Market Participant (FRMP) for the security service asset, the service provider must ensure the FRMP has been notified that the asset will be used to provide system security services, and to ensure the FRMP (as the PA), has assigned system access accordingly.

The following SSM entities should be used when assigning users with the appropriate level of access (i.e. create, read, update):

1. SSM Access for Availability Screen
2. SSM Access for Enablement Screen

Non-registered Participants

A non-registered participant means the entity/person is not a Registered Participant per the NER *definition 'a*

person who is registered by AEMO in any one or more of the categories listed in rules [NER] 2.1A to 2.7.'

In order for non-registered participants to gain access to the SSM Application through the AEMO Markets Portal, a private data network connection to MarketNet must be established and details of a designated PA contact provided.

AEMO's Support Hub coordinates both requests and can be submitted via the phone number or email outlined below.

For the VPN connection request, please ensure you specify that you are a Security Service Provider requiring a non-market non-code variable VPN.

Note the timeframe to set up a new MarketNet Connection is up to four weeks.

When providing the PA details, please note they must be an IT contact and must be authorised by a person within the business who has the appropriate level of authority, such as the CEO or an equivalent senior executive.

AEMO Support Hub Contact Information

Phone: 1300 236 600
Email: supporthub@aemo.com.au

Please ensure that opstransition@aemo.com.au is cc'd on all correspondence to Support Hub.

Once the PA profile has been created, it is their responsibility to assign the appropriate user access via the User Right Management tool. For a guide on how to do this, please refer to the AEMO Guide to User Rights.

The following SSM entities should be used when assigning users with the appropriate level of access (i.e. create, read, update):

1. SSM Access for Availability Screen
2. SSM Access for Enablement Screen

Note: service providers using Network Outage Schedule (NOS) must ensure they have communications protocol in place with the relevant TNSP in managing their availability.

What SSM Market Portal functions will be used and tested?

During system preparedness testing, service providers will be required to perform the following in the pre-production environment:

- Log into the SSM interface or API using credentials issued by AEMO.
- Access the SSM interface to view contract details.
- Submit Availability:
  - Methods: Manual edit, Quick Fill, Row duplication, CSV/JSON file upload.
  - Note the availability data must be submitted up to 7 days ahead and current and next 30-minute trading intervals cannot be edited.
- View Enablement Instructions: Instructions issued by AEMO will be visible in the Enablement Instruction screen of the SSM interface.
- View Day+1 enablement and cost reports.

What to expect in system preparedness testing?

Note: These tests are system-only and non-operational and do not require service providers to physically run their units.

As part of the system preparedness testing, service providers will be asked to:

- Update and maintain unit availability data and operational parameters via the SSM interface or API.

- Confirm receipt and visibility of test enablement instructions.
- Verify receipt of amended and cancelled instructions.
- Confirm visibility of daily enablement reports and access to ISF private reports.

System Preparedness Checklist

This checklist summarises the key activities that service providers will be required to complete during System Preparedness Testing. Service providers will be required to confirm completion of these activities by submitting screenshot evidence via email to AEMO's Operations Transition team (opstransition@aemo.com.au).

Activity	Market Portal	API	NOS
Confirm access to market portal / API portal in pre-prod environment	☐	☐	N/A
Confirm communications protocol in place for NOS reporting	N/A	N/A	☐
Confirm phone access with AEMO	☐	☐	☐
Confirm availability data can be uploaded and updated	☐ (manual, quick fill, row copy, CSV/JSON)	☐	N/A
Confirm visibility of availability data	☐	☐	N/A
Confirm receipt and visibility of enablement instructions	☐	☐	N/A
Confirm receipt and visibility of updated enablement instructions	☐	☐	
Confirm reporting access for day+1 reports	☐	☐	N/A

What are service provider responsibilities in system preparedness?

- Ensure authorised staff can access the SSM interface / API.
- Maintain and update unit availability during testing.
- Confirm receipt and visibility of enablement instruction.
- Report any issues to AEMO Ops Transition via opstransition@aemo.com.au

Next Steps:

After successful completion of system readiness by the service provider, a confirmation email will be sent to the TNSP, informing the contract has been flagged as ready for live enablement in the production environment.

Where can I find more information?

See AEMO's website for ISF related documents and Security Enablement Procedures here.

See the AEMC's website for the *Improving security frameworks for the energy transition (ISF) rule change final* determination.
For any further enquiries, please contact AEMO's Operations Transition team via:

- **Email:** opstransition@aemo.com.au or

Alternatively contact the AEMO Support Hub on

- **Phone:** 1300 236 600
- **Email:** supporthub@aemo.com.au

This fact sheet is only a summary of the system preparedness testing. The service providers are responsible for ensuring they understand the relevant provisions of the National Electricity Rules and other applicable instruments, which prevail in the case of any inconsistency.