DEIP Standards, Data and Interoperability Working Group

Meeting 1 – 22 April 2020

Agenda

1. Welcome & Introductions

2. Overview of the Working Group
   a. Purpose
   b. Membership
   c. Governance Structure

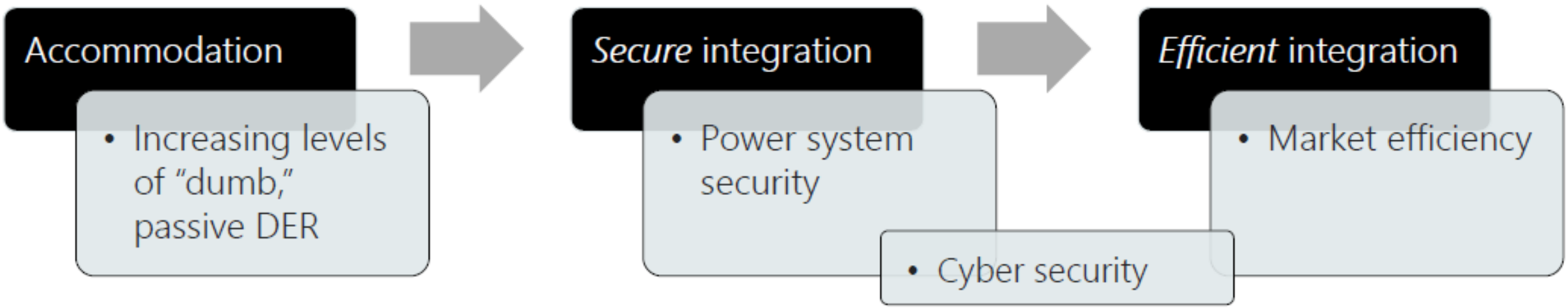
3. Overview of proposed rule change proposal for Minimum DER technical requirements

4. Technical Working Groups
   a. Device and Performance standards
   b. Cyber Security
   c. APIs and Data Standards
      i. API Working Group – ANU
      ii. Data – Solar Analytics

5. Workplan Priorities

6. Meeting Summary
   a. Agreed Actions & Next meeting

Where we are today and… where we want to get to



Approach to date with Air conditioners and PV

Urgent short term actions for requirement for power system security.

Trials today and medium-to-longer term actions to co-optimise DER with the larger power system.

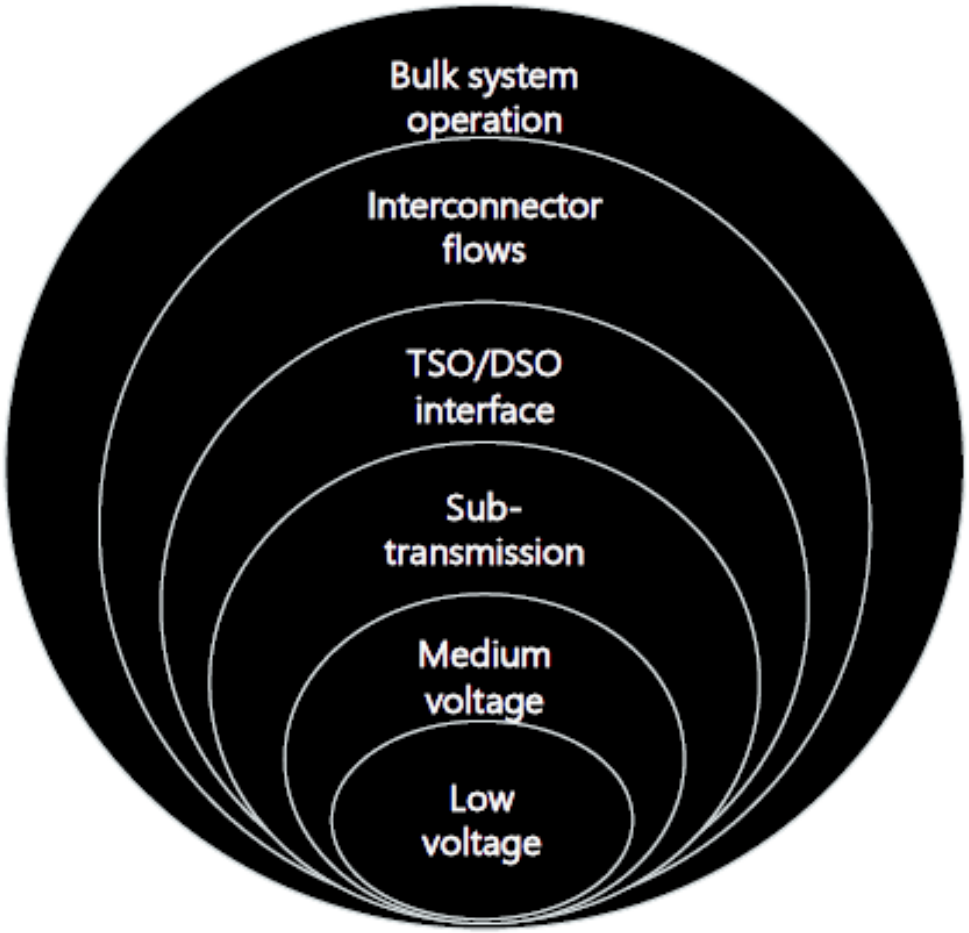
Why accommodation of passive, dumb devices is a problem…

Performance not aligned with power system needs.

Largely passive, not controllable by system operator.

Growing aggregate impact as penetrations increase, compromising AEMO's ability to securely operate the bulk power system.

System implications



Increasing penetration of passive DER

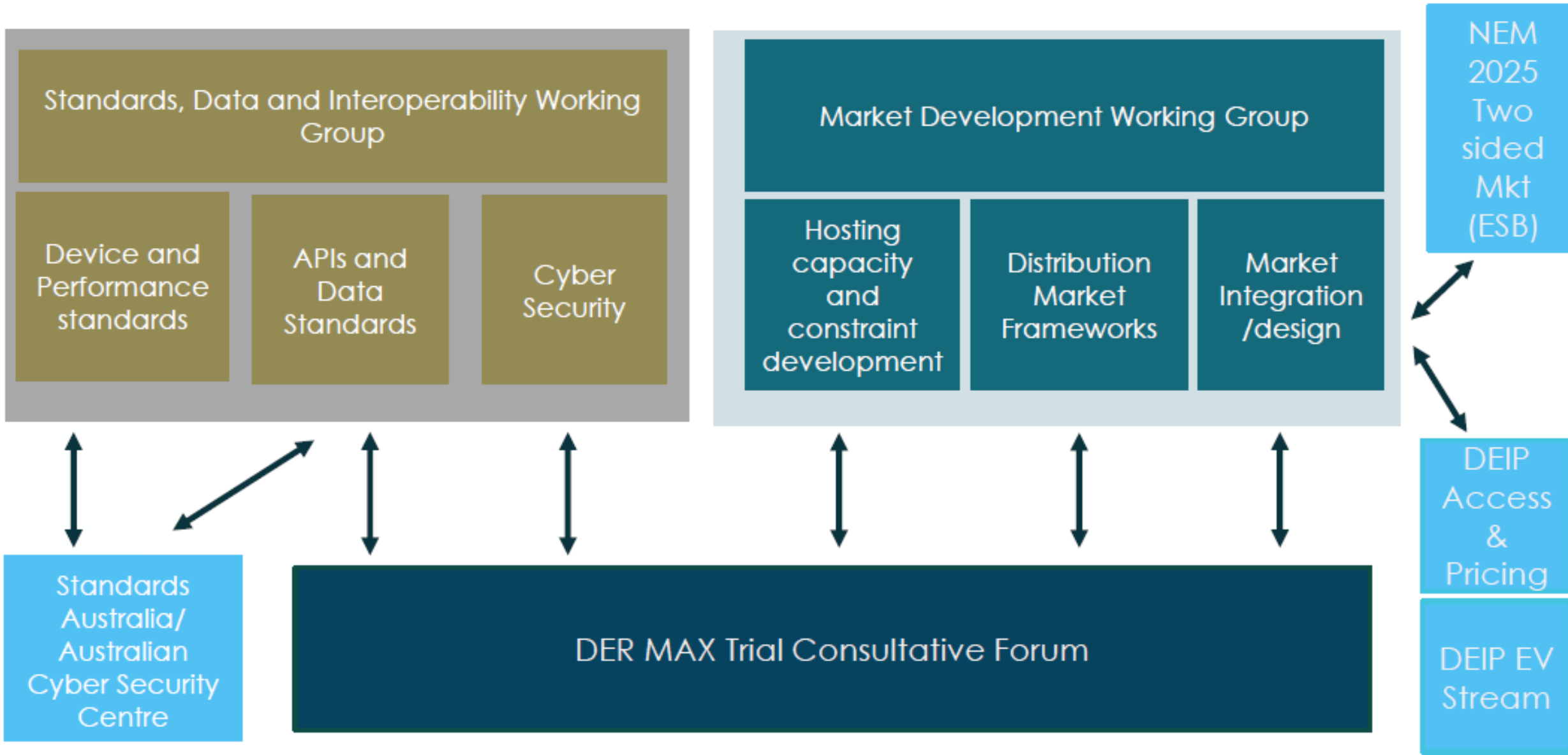
Core duties of the bulk system operator are impacted with high DER in aggregate across regions, including: system balancing, stability, recovery and restoration following major system events.

Issues arise at the transmission-distribution interface such as congestion due to reverse flows, voltage control challenges, managing stability and other limits.

Limitations arise in the distribution network, typically steady state over-voltages, thermal limits, short circuit level, protection coordination, power quality, and islanding risks.

Low levels of passive DER participation is not typically a problem and relatively easily accommodated within the distribution network with little restriction or intervention.

Market and Standards Working Groups



DEIP Standards, Data and Interoperability Working Group

The role of the SDIWG will be to provide oversight, and help align, steer and coordinate the taskforces focused around key activities to update Standards for devices, connections, communications and cyber security to support DER integration and where appropriate feed key design elements into each of the trials..

The objective of the working group will be to:

- Review current governance arrangements for DER standards, connections, operations to determine key gaps and escalation points.
- Endorse scope and membership and define any technical working groups on specific issues
- Ensure appropriate stakeholder consultation and co-design opportunities
- To provide resources as appropriate to each technical working group
- Help define the key design elements of the DER Max set of trials
- Socialise within own organisation and represent to the wider DEIP stakeholder community
- Help to ensure efficient and effective interactions with other DEIP streams (eg. Markets, Access and Pricing and EVs)
- Recommend new activities and collaboration opportunities
- Escalate any issues to the DEIP Steering committee as appropriate

SDIWG Purpose

1. Provide steering to the technical working groups focused around key activities already underway to update Standards for devices, connections, communications and cyber security to support DER integration and where appropriate feed key design elements into each of the trials.

2. Co-ordinate, communicate and steer the activity that will form the key components of the data and interoperability of devices in the distribution network, in the process look to ensure standardisation of communication, technical device operations and integration of DER with the wholesale, FCAS and network services markets.

SDIWG Purpose cont.

3. Not being a formal governance body may need from time to time to refer key items for decision to other bodies; this may include Standards Australia or equivalent, DEIP Steering Group, ESB, the Australian Cyber Security Centre or the energy market rules consultation process.

4. The SDIWG key task initially will be to define the current standards, data and interoperability landscape, and highlight key priority areas and to communicate this with the DEIP Steering Group and broader stakeholders.

SDIWG Scope

The Scope of the group will be to steering the Market Development and Interoperability Streams of the Distributed Energy Integration Program as well as steering/reference group for the DER Max national program of DER trials.

Membership

The initial SDI Working Group will consist of the following core members:

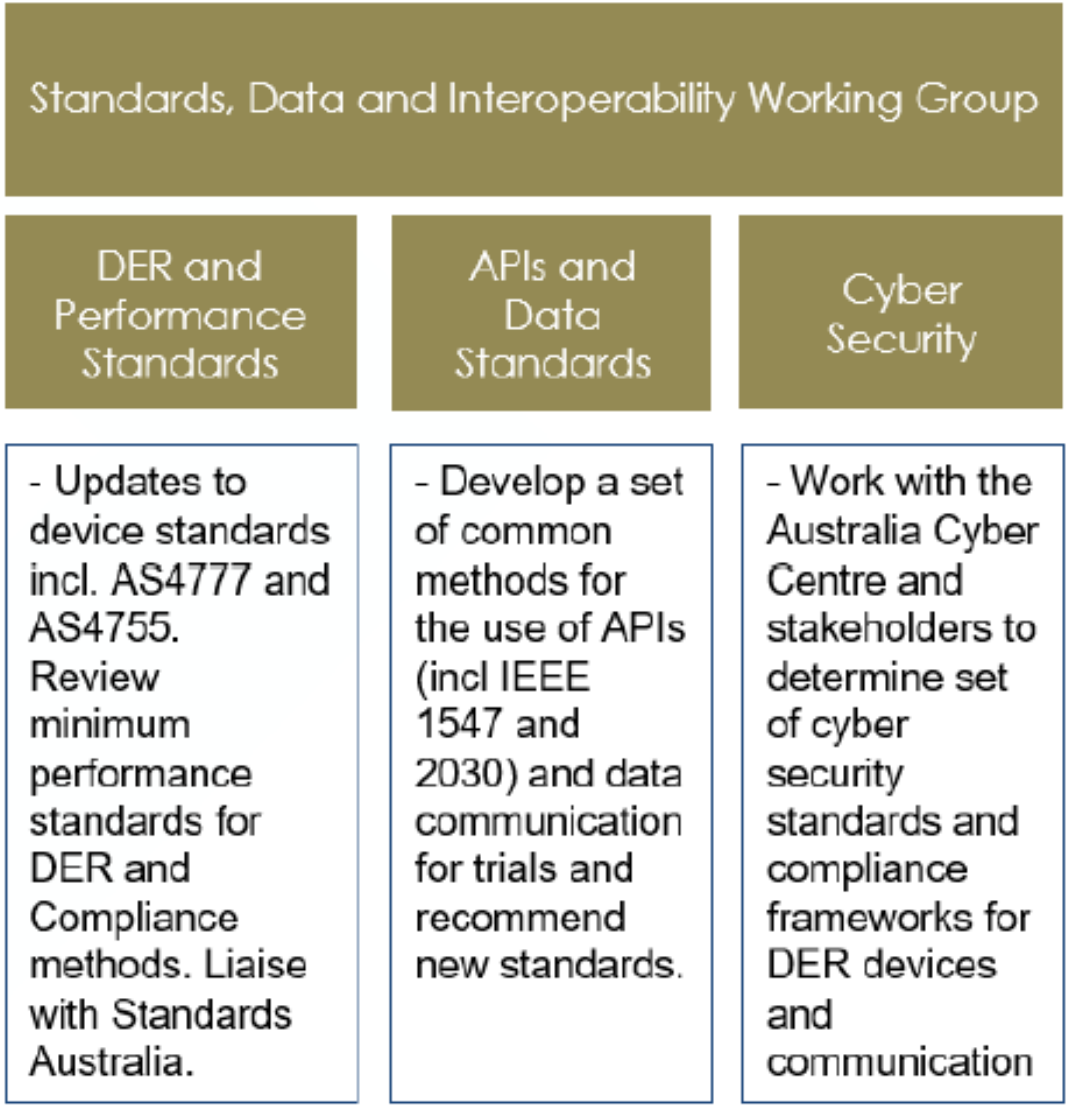
The core membership may also expand, as their may be a need to add further supporting members (non-voting) to the steering group as the need arises and at the instigation and decision of existing members.

Type	Organisation
Core	AEMO
	AER
	AEMC
	ARENA
	CEC
	ENA
	ECA
	CSIRO
	AEC
	Smart Energy Council
Tech Working Group Chairs	Device and performance standards
	API and Data
	Cyber Security

SDIWG Structure

There will be three working groups under SDIWG Initially, and each will be to some extent formalising work already underway in each of the specific subject areas identified.

Key stakeholders will be installers, networks and AEMO, as well as the customers who own DER and their agents responsible for integrating it into the Network and wholesale Market.



Technical Working Group Membership

It is proposed that we would align with Standards Australia and current Standards Australia technical committees where applicable

DER and Performance Standards	APIs and Data Standards	Cyber Security
- AEMO, DNSPs, ENA Universities, CSIRO, CEC, Standards bodies, Device Manufacturers and Device Installers and Integrators	- AEMO, CEC, DNSPS,ENA ARENA, Aggregators, Retailers, Device Manufacturers, Installers and Integrators. Incorporate various other ARENA funded project activity.	- AEMO, DNSPs, ENA ARENA, CEC, Australia Cyber Centre, other state and federal bodies. Device Manufacturers, Installers and Integrators

Meetings

Meeting frequency: SDIWG will meet monthly. Working Group members will define the meeting frequency of their meetings.

Meeting papers: AEMO will endeavour to provide advice and all meeting documentation prior to each meeting.

Meeting notes: AEMO will endeavour to circulate any meeting notes and outcomes within five business days after each meeting.

Overview of proposed rule change proposal for Minimum DER technical requirements

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Technical Working Groups

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

API & Data Technical Working Group

Lachlan Blackhall - ANU

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Cyber Security of Distributed Energy Resources: Technical Working Group

Terms of Reference (ToR)

Terms of Reference (ToR)

The purpose of these terms of reference is to establish the working arrangements for this group.

Role / Purpose	The role of the Cyber Security of DER: Technical Working Group is to coordinate and implement consistent cyber security capabilities across Australia's DER ecosystem. Members of this group are responsible for developing a DER cyber security platform across the energy industry, and application of the technical standards and frameworks required to deliver this outcome. The technical working group will: • Review the cyber security capabilities required to protect the DER ecosystem and develop standards / framework as required to formalise this • Collaborate and design the DER Cyber implementation blueprint • Develop across market 'participants' the standardised interface / systems required to deliver these capabilities; developing a cyber security platform that functions across all sectors of the energy industry • Establish and lead specific sub-working groups to implement the capabilities across the sector of the energy industry Working Group members represent.
Term	This Term of Reference is effective from (xx/xx/xxxx) and continues until Working Groups members consider the outcomes have been achieved as determined by 80 per cent group majority.

Terms of Reference (ToR)

Membership representatives	The Cyber Security of DER: Technical reference group will consist of technical members knowledgeable in cyber security frameworks, distributed energy resource devices, implementation of cyber security platforms within their jurisdictions: The desired attributes of members of the group are: • Minimum 5 years in energy with cyber security working reference • Broad knowledge of cyber security frameworks, design and implementations • Knowledge of DER devices and their capabilities • Understanding of blockchain technology, network security, risk management, security operations, data security • Experience in technical working reference groups • Cyber security qualifications from recognised Australian / International organisations

Terms of Reference (ToR)

Membership representatives

The Cyber Security of DER: Technical reference group will comprise of

Name	Title	Reference Group Role	Organisation
Matthew Hyde	DER Program - Standards Stream Lead	Member	AEMO
Pearse Courtney	Project Manager - Industry Framework Establishment - Cyber	Member	AEMO
David Bradshaw	Enterprise Security Architect	Member	AEMO
TBA	PMO Project Administrator	Secretariat	AEMO

***Non-members may be invited to attend group meetings as either a nominated proxy or in cases to present information.*

Terms of Reference (ToR)

Roles and Responsibilities	The Cyber Security of DER: Technical reference group are **accountable** for: • Fostering collaboration and robust discussion and debate • Limiting the obstacles to the groups' successful delivery, adoption and use of standards • Maintaining the focus of the group in agreed scope, outcomes and benefits • Monitor and managing factors outside the technical reference groups control that are critical to its success The Cyber Security of DER : Technical reference group **members will commit to**: • Attendance at all scheduled Cyber Security of DER: Technical reference group meetings, or nominate a proxy • Engage in constructive, open and frank discussion in bringing a members perspective to group discussion • Work together in a manner with other members and other representatives associated with the group ethically with courtesy, respect and integrity • Represent fairly and responsibly and act in the best interests of their industry • Review of cyber security capabilities and standard materials provided • Developing across market 'participants' the standardised interface /systems required to deliver cyber security capabilities; developing a cyber security platform that functions across all sectors of the energy industry • Willingness to be a conduit for peers in their industry and or market segment to provide input and feedback back to the group. (establish and lead specific sub-working groups to implement cyber security capabilities across the sector of the energy industry working group members represent). • Share all communications and information across all members of the Cyber Security of DER: Technical reference group • Notify members of the Cyber Security of DER: Technical reference group, as soon as practical, if any matter arises that is deemed to affect the groups objectives of what it is set out to achieve The Cyber Security of DER : Technical reference group **members will act with due diligence**: • Not use their membership for any commercial advantage, including marketing or access to privileged information • Each person who represents a company or organisation on the group is responsible for making their company or organisation aware of the responsibilities associated with the membership of the group • Members will declare any conflict of interest to the secretariat

Terms of Reference (ToR)

Roles and Responsibilities	The Cyber Security of DER: Technical reference group **members expectations** are: • Each member will be provided with complete, accurate and meaningful information in a timely manner • To be given reasonable time to research, analyse and provide key information back to the group • To be alerted to potential risks, issues, constraints that could impact the technical reference groups objectives as they arise • Open and honest discussions, without resort to misleading assertions • On-going quality monitoring to verify the overall status and health of the technical reference group The Cyber Security of DER: Technical reference group **members will adhere to:** <u>Confidentially</u> Members must regard all information made available to them in agendas, minutes and all discussions at the Cyber security DER: Technical reference group as confidential until informed otherwise by the Chairperson. Members may receive information that is regarded as 'commercial-in-confidence', confidential, have privacy implications. Members acknowledge their responsibility to maintain confidentially of all information that is not in the public domain. <u>Conflicts</u> Upon becoming aware of a conflict of interest, members and attendees must immediately declare their conflict of interest to the Chairperson, who will exclude them from discussions and decisions that put the member in conflict. Where the conflict excludes the member from a significant amount of the Cyber Security DER: Technical reference groups role and purpose, the Chairperson may request the member to resign from the group.

Terms of Reference (ToR)

Meetings	• All meetings will be chaired by AEMO
	• A meeting quorum is defined as 6 members of the technical reference group
	• Topics for meetings will be discussed at the meeting prior for inclusion in the future meeting Agendas
	• Meeting formats may include demonstrations, workshops, presentations, questions and answers sessions, group work
	• The Secretariat – AEMO will provide to all members:
	  • Meeting Agendas
	  • Meeting Minutes
	  • Meeting schedule for the term
	• Meetings will be scheduled monthly for 2 hours at AEMO ….. Brisbane etc … until the end date of the term.
	• Meetings will be conducted face to face with web conference facilities also available.
	• Meetings may also occur "out of session" at the discretion of the chair. In this event, notification will be communicated as soon as practical
	• Meeting attendance will be registered
	• Decisions on actions will be made by consensus (members are satisfied, even if it is not their first preference)

Data and Information share	• All meeting minutes, supporting papers, resources, registers, and confidential materials shared by the Cyber Security DER: Technical reference group will be accessed and stored in a central password protected repository. • All members will have access to the repository to review and store materials. • AEMO will be accountable and responsible for the support and maintenance of the repository
Amendment , Modification or Variation	These terms of reference may be amended, modified or varied in writing after consultation and agreement by the Cyber Security DER: Technical reference group members.

Short Term Work Priorities

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Aspect	Area	Action
Device capability and performance	Bulk power system disturbance withstands and autonomous grid support. Interoperability – the ability of the device to be communicated with and follow commands.	**Q2 2020 (technical requirements):** ratification of AS4755.2 for demand response for selective types of residential electrical products (Air Conditioners, Pool Pump Controller, Hot Water Systems and Storage/Battery Systems). **[national]** **Q1 2021 (collaborate):** fast track short duration voltage disturbance ride-through capability for all new DPV inverters. Require compatible existing DPV fleet that already complies to be listed in a separate register. **[SA and WA, others encouraged]** **Q1 2021 (collaborate):** establish device level requirements for emergency control of new DPV systems. Examine non regulatory mechanisms to encourage adoption in compatible existing fleet. **[SA and WA, others encouraged]**
Aggregation and control	Emergency curtailment	**ASAP (collaborate):** engage with DNSPs to establish emergency control of commercial-scale DPV systems. **[national]** **Q2 2021 (collaborate, trial):** trial and establish NSP implementation pathway for minimum emergency control capabilities of DER (including loads and generation) via Advanced Metering Infrastructure (AMI). **[SA and WA, others encouraged]**
	Dynamic control for DER aggregations	**Q2 2021 (technical requirement, Rule change):** Establish power system security requirements for aggregations to be made mandatory when registration and market participation rules are established in the NER. **[national]**
Data and information exchange	Static data for planning and forecasting	**Q2 2021 (collaborate, Rule change):** provision for EVs and controllable loads to be included in the DER register. **[national]**
	Operational visibility, observability and predictability	**Q4 2020 (collaborate, technical requirement):** establish consistent real-time SCADA for all non-scheduled generation in the 100kW to 5MW size range. **[national]** **Q2 2021 (trial, technical requirement):** establish minimum real time visibility/predictability requirements for DPV systems available for emergency curtailment. **[national]** **Q2 2021 (collaborate, technical requirement):** establish consistent structure requirements for DER and LV network monitoring data so it can be readily used by DNSPs and in the assessment of standards compliance. **[national]** **Q2 2021: (collaborate, technical requirement):** establish consistent data structure requirements for data collected by AMI and behind-the-meter data vendors so this can be more easily utilised. **[national]**
Cyber security	DER cyber security requirements	**Q2 2021 (collaborate, technical requirement):** establish DER cyber security threat model and roles and responsibilities and articulate to market. Develop a DER cyber security framework / standard to mitigate / detect the identified threats. **[national]**
Governance	System security requirements within Standards and other instruments.	**ASAP (Rule change):** Take forward a rule change proposal that provides AEMO the regulatory powers to mandate uniform DER power system security requirements for connected DER. Establish how power system security needs are prioritised and included within Australian Standards set by industry consensus. **[national]**.
	Governance structures to improve compliance with standards.	**Q4 2020: (collaborate):** work within ESB governance review to ensure supporting governance structures and mechanisms are in place for high DER future. **[national]**

Meeting Summary

Agreed Actions & Next meeting

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR