

NEM Summer Preparedness

Cyber briefing

Tim Daly
Jason Smith

GM Cyber Security
Manager Energy Market
Cyber Coordination

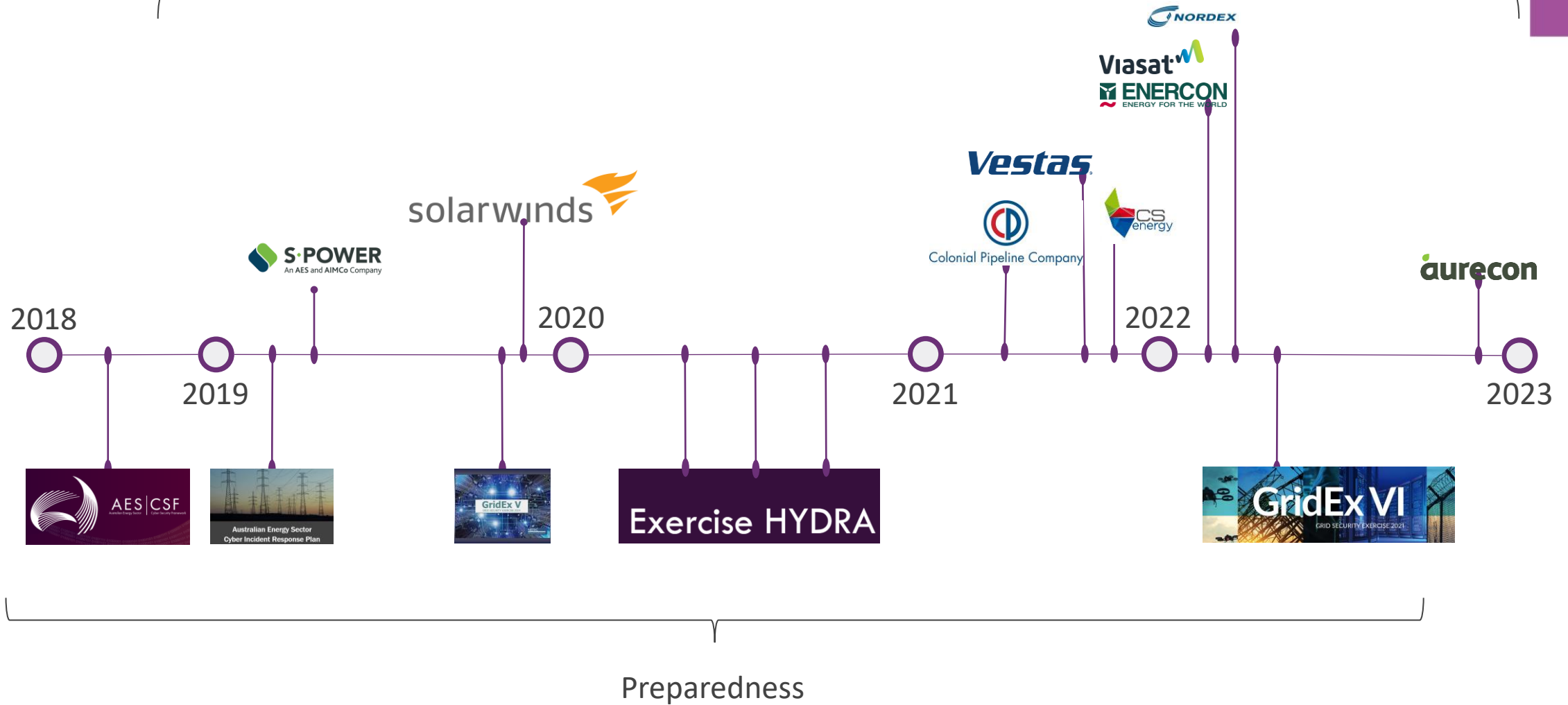


Agenda

1. Evolving energy sector cyber threats
2. Australian Energy Sector Cyber Incident Response Plan (AESCIRP)
3. Energy Market Cyber Coordination (EMCC)
4. Upcoming activities

A brief history

Publicly reported
energy cyber incidents



Shields Up!



TLP: WHITE

Australian organisations should urgently adopt an enhanced cybersecurity posture

Entities should follow ACSC advice and improve their resilience within a heightened threat environment.

Version: 11 Last Updated: 28 April 2022

Prioritise these actions to defend against malicious cyber activity

Organisations should prioritise the following actions to mitigate against threats posed by a range of malicious cyber actors. Many actors use common techniques such as exploiting internet-facing applications and spear phishing to compromise victim networks. Organisations should ensure they have implemented mitigations against these common techniques and are prepared to detect and respond to cyber security incidents. The following four actions will improve an organisation's resilience in the current threat environment.

1. Patch applications and devices, particularly internet-facing services. Monitor for relevant vulnerabilities and security patches, and consider bringing forward patch timeframes.
2. Implement mitigations against phishing and spear phishing attacks. Disable Microsoft Office macros by default and limit user privileges. Ensure that staff report all suspicious emails received, links clicked, or documents opened.
3. Ensure that logging and detection systems are fully updated and functioning. Prioritise internet-facing and critical network services, and ensure that logs are centrally stored.
4. Review incident response and business continuity plans. Plan responses to network compromise as well as disruptive or destructive activity such as ransomware. Ensure these plans are known to and actionable by staff, and are accessible even when systems are down.

Organisations should also review the Essential Eight and prioritise remediating any identified gaps in Essential Eight maturity. Following this, organisations should review technical details associated with any specific threats they have identified as relevant and incorporate these into monitoring and response plans.

Russian state-sponsored and criminal cyber threats to critical infrastructure

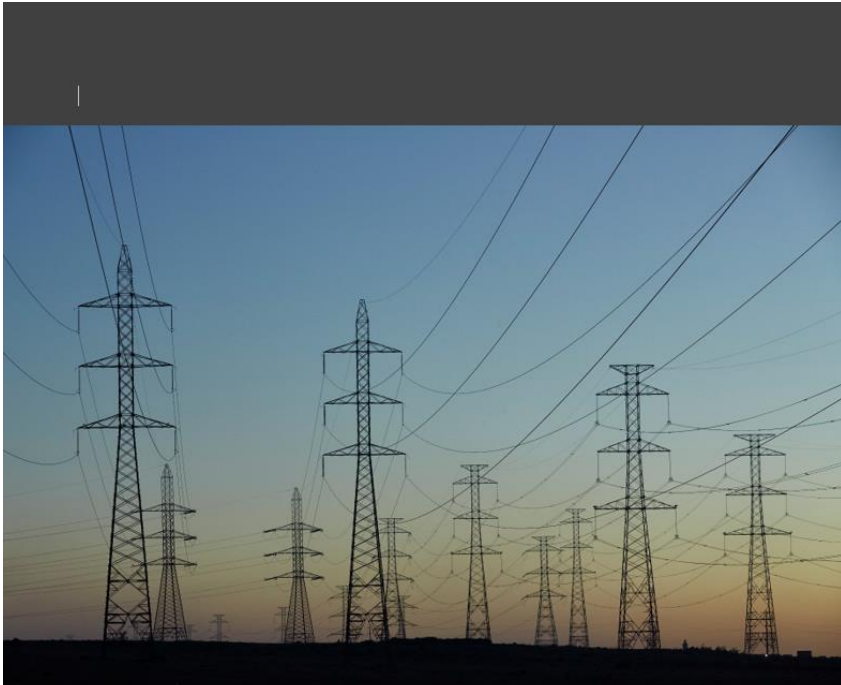
A [joint cybersecurity advisory](#) has been coauthored by U.S., Australian, Canadian, New Zealand, and UK cyber authorities, with contributions from industry members of the Joint Cyber Defense Collaborative (JCDC), which provides an overview of Russian state-sponsored advanced persistent threat (APT) groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

Australian critical infrastructure organisations should review the technical details, mitigations, and advice provided in this [joint cybersecurity advisory](#).

ACSC Threat Report



Australian Energy Sector Cyber Incident Response Plan (AESCIRP)



**Australian Energy Sector
Cyber Incident Response Plan**

Interim National Electricity Market Plan

Report cyber security incidents to the
Australian Cyber Security Centre on 1300 CYBER1 (1300 292 371).

Report cyber security incidents to your
Australian Energy Market Operator Cyber Duty Manager on 0455 725 219.

If you are concerned about your immediate safety or there is a threat to life,
you should contact 000 immediately.

Cyber Incident
Management
Arrangement
for Australian
Government

CIMA

	Low Severity (LS)	Medium Severity (MS)	High Severity (HS)	
Information compromise	1	14	28	
Service compromise	4	28	72	75
Controlled loss of service	4	116	146	137
Uncontrolled loss of service	1	29	35	62

Incident
categorization
matrix

POWER SYSTEM EMERGENCY
MANAGEMENT PLAN (PSEMP)

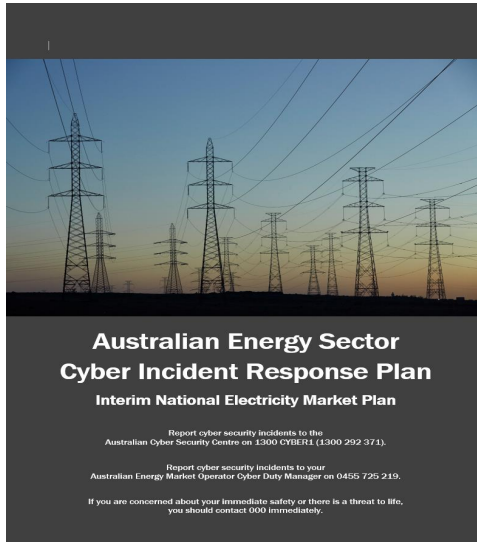
PSEMP

CONFIDENTIAL-RESTRICTED CIRCULATION

Energy Market Cyber Coordination



Energy Market Cyber Coordination



- Newly created and dedicated function
 - Initial focus on sector level cyber incident response coordination arrangements
 - Accountable for managing the AESIRP and the Cyber Duty Manager role
 - Ensuring market standards and participant agreements include appropriate security obligation
- Pending Energy Minister's endorsement could also:
 - Manage AESCSF lifecycle and reporting
 - Coordinate research on emerging cyber security threats to the energy sector
 - Promote shared awareness of cyber threats to the sector

EMCC Upcoming activities



- Validating operational cyber contacts
- Jurisdictional engagements to further exercise AESCIRP and to explore State specific cyber arrangements
- Planning for multijurisdictional engagement noting GridEx VII scheduled for November 2023

Closing takeaways

- Confirm that your organization has access to the AESCIRP and that the Cyber Duty Manager contact details are included in your operational response plans
 - email emergency@aemo.com.au to get a copy of the AESCIRP
 - CDM contactable 24/7 on **0455 725 219**
- Expect validation of operational cyber contacts by AEMO in the coming months
- Consider how you will participate in cyber exercises for 2023
- We will be seeking market participant involvement in upcoming initiatives