


ROADMAP FOR STANDARDS AND GRID CYBER SECURITY

Final Report December 2018



About this Report

The roadmap for Standards and Grid Cyber Security (Roadmap) was prepared by Standards Australia and identified by Energy Networks Australia (formerly Energy Networks Association) (ENA) as a fundamental enabler to support the digitalisation and decentralisation of the distributed energy system. It is crucially linked to the ENA/ Commonwealth Scientific and Industrial Research Organisation (CSIRO) Electricity Network Transformation Roadmap published in 2017.

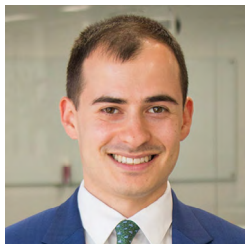
The Roadmap aims to support existing government and regulator projects such as “Cyber Security Industry Uplift” which involves Australian Energy Market Operator (AEMO), Australian Signals Directorate and the Department of Home Affairs.

Standards Australia acknowledges the financial support from ENA for this Roadmap as Standard Australia’s co-resourcing partner.

Co-resourcing partner:



Report Author



Michael Paparo
Policy Manager
Standards Australia

@ | michael.paparo@standards.org.au
📞 | 0439 657 795

More Information

Michael Paparo is the Policy Manager responsible at Standards Australia for the Grid Cyber Security Standards Project with Energy Networks Australia.

Prior to joining Standards Australia, Michael worked in public policy at the Property Council of Australia, Chamber of Commerce & Industry Queensland (CCIQ), and as an official at the Commonwealth Treasury Department in Canberra.

Michael holds a Bachelor of Economics and Bachelor of Arts from the University of Western Australia and is currently based in Sydney, Australia.

Acknowledgements

This report benefitted from significant inputs and insights provided to Standards Australia by the staff at Energy Networks Australia.

Useful comments and suggestions on various aspects of this report and roadmap were provided by Mr Heath Frewin and Dr Stuart Johnston both of Energy Networks Australia.

About Standards Australia

Founded in 1922, Standards Australia is an independent, not-for-profit organisation, recognised by the Commonwealth Government as the peak non-government standards development body in Australia. It is charged by the Commonwealth Government to meet Australia's need for contemporary, internationally-aligned standards and related services. The work of Standards Australia enhances the nation's economic efficiency, international competitiveness and contributes to community demand for a safe and sustainable environment.

www.standards.org.au

Foreword



Dr Bronwyn Evans,
Chief Executive Officer,
Standards Australia

The energy and electrotechnology industry in Australia is rapidly evolving with the application of digital technology to traditional infrastructure. This is leading to changes in business models, physical infrastructure requirements and at the same time presenting new security challenges for operators, business and consumers. Developments in electrical storage, new types of generation, the emergence of the 'Internet of Things (IoT),' changes in consumer preferences, and other drivers are encouraging innovation and adaptation of existing infrastructure to support these new demands and directions. Adaptations include the shift from the traditional centralised structure to a more decentralised approach has given rise to a new generation of energy providers called 'prosumers' who both consume electricity and produce it; and may sell excess energy from their premises back into the grid.

The electricity grid evolution includes greater information and communications technology (ICT) to monitor and perform real-time control. As a result, the integration of computing and communication capabilities opened the distributed energy grid to new vulnerabilities which have the potential to allow cyber attackers to inflict damage and disruption to critical infrastructure and management systems.

The Roadmap is the outcome of a structured program of consultations aimed at strategically identifying standardisation efforts over the short, medium and long term. The consultation brought together a broad range of stakeholders who have an interest in cyber security of the grid, enabling conversations between key groups, and finally setting out a list of prioritised actions to guide future directions in grid cyber security.

Contents

About this Report.....	2
Acknowledgements.....	3
Foreword	4
Executive Summary.....	6
Background	7
Key topics/functional areas.....	8
Consultation Approach.....	11
National Consultation and National Forum.....	11
Action Plan	15
Conclusion.....	18
Appendix A- Industry Workshop	19
Appendix B: Action Plan Committees.....	20
Appendix C: Standards Overview.....	23

Executive Summary

As the distributed electricity system continues to evolve from a centralised model towards a decentralised system the risks of cyber security need to be addressed.

The Roadmap was produced as a result of a discussion paper, national forum and stakeholder consultations (March 2018 to October 2018). This enabled industry, consumer and government to express priorities and identify relevant international standards committees and standards for engagement by Australia.

The Roadmap is an informative tool for stakeholders that recognises the importance of allowing the development of markets and business while providing support through future standards development. The agenda of Standards Australia and the program of work it undertakes is driven by stakeholders, including industry organisations, network operators, other market participants and indeed regulatory agencies and relevant government departments. It is therefore critical that the recommendations of the report be driven by key industry and government stakeholders so that standardisation gaps can be closed.

The Roadmap has identified the need to engage internationally, particularly with a number of Systems Committees and Technical Committees at the International Electrotechnical Commission (IEC). Policies that drive international standards participation will ensure that Australia's perspectives are incorporated at this level, facilitating the potential national uptake of standards produced by these groups.

These groups have been identified by stakeholders as key resources supporting cyber resilience of the grid. Through collaboration of government, industry and relevant stakeholders, Australia can take advantage of the opportunities identified in this report.

The Roadmap was written with input from stakeholders and supports a recommendation of the Network Transformation Roadmap undertaken by ENA and the CSIRO.

Key insights of stakeholder consultations include:

- Stakeholders agreed that internationally aligned cyber security standards for the energy grid are of crucial importance not only for energy companies but also for consumers, retailers and the broader economy in Australia.
- Stakeholders agreed for the national uptake of trusted international standards as key resources supporting the transformation of the grid and cyber resilience.
- Stakeholders identified key areas of current vulnerability for the grid including:
 - Structural change of the grid with greater interconnectivity;
 - Industrial Internet of Things (IIoT);
 - Building management systems (BMS);
 - Increased convergence between Operational Technology (OT) and Information Technology (IT); and
 - The rise of cybercrime.
- Emerging themes such as data management and privacy must be managed at both the technical standards and policy level to ensure trust is maintained in the energy grid.
- Including best practice and standardisation efforts in cyber security from other sectors of the economy such as financial services and information technology will help support cyber security of the energy grid.

Key recommendations of this Roadmap include:

- The development of standards and documents to support grid cyber security in Australia including workforce screening;
- Australian participation on relevant international standards committees; and
- Reviewing the membership and terms of reference for a number of relevant Australian Technical Committees.

These recommendations will help to address the challenges of grid cyber security supporting the energy transmission industry to raise cyber maturity levels as it evolves and becomes increasingly decentralised and digitalised.

Background

The Grid Cyber Security Roadmap represents an important component of the larger framework of the joint Electrical Network Transformation Roadmap between Energy Networks Australia (ENA) and the CSIRO. The Roadmap's stated objectives are:

In this time of unprecedented change for global energy services, the Roadmap is designed to identify the preferred transition which the electricity network industry must make in the next decade, to be ready to support better customer outcomes under a diverse range of long-term energy scenarios.

By setting out a pathway for the transition of electricity networks by 2025, the Roadmap seeks to position network businesses and the whole energy supply chain for the future. The Roadmap also intends to support the evolving needs of customers, innovate and develop new services that customer's value and foster the long-term resilience and efficiency of Australia's energy system.

Stage 1 of the ENA/CSIRO Roadmap identified standards as one important enabler to realise the various potential "futures" of the grid. Please see Figure 1 for a graphical representation of a future energy system. Standards play a key role in enabling more interactive power systems by supporting operations between technologies, providing consistent frameworks for design and implementation and ensuring safety and security of supply. In fact, the integration of new technologies and distributed energy resources (DER) and interoperability will be fundamental to the performance of the power system of the future.

The challenges and potential future gaps in cyber security of the energy grid were also identified in Standard Australia's [Roadmap for Standards and the Future of Distributed Electricity](#) published in May 2017 which was co-resourced with CSIRO and ENA.

The role of standards

Currently a number of existing international, regional and national standards are used by industry to provide protection of the grid and supply chain. These standards include functional areas such as market systems and operations, governance and services, generation, transmission and distribution, prosumers and data.

While the Government sets Australia's legislative and regulatory framework, Australian and international standards play a crucial role in supporting the broader institutional architecture. Standards enable and support Australian industry to engage with, and benefit from, the digital economy. Standards enable business to boost efficiency, increase productivity and maximise growth.

In the energy and electrotechnical sectors, standards play a key role in supporting interoperability between technologies, providing consistent frameworks for design and

implementation, and ensuring safety. For example, the Australian and New Zealand Wiring rules provide a foundation for the electrical installation industry, and the development of standards which supported the growth of the rooftop solar industry in Australia.

Standards Australia is able to have a greater say and influence on international standardisation activities at the ISO and IEC as Australia's representative at these organisations. Whereas Standards Australia is not Australia's member of IEEE and other international standardisation organisations and therefore unable to influence the direction of future energy cyber security standardisation activities at these organisations.

Key topics/functional areas

Standards Australia conducted consultations from March 2018 to October 2018 across Australia with stakeholders from government, regulators, industry, academia and consumer groups on grid cyber security and the role of standards. Five key topics/functional areas were identified in this process which are listed below.

Please see Appendix C for information regarding relevant Australian and International standards committees and standards.

Infrastructure Resilience

A critical factor in keeping the energy grid secure from malicious intent is ensuring that the infrastructure supporting the grid is resilient. For this reason, it is important that the design and construction of critical infrastructure, such as those used to generate, transmit and distribute energy is secure and resilient. At the moment, there is limited standardisation activity happening in this space with the most recent activity being on microgrids.

Subtopics:

- Energy Supply (generation, transmission and distribution)
- Microgrids
- Assets and Facilities Management

Network and Power Systems Communications

As the energy grid transitions from a 'one-way' power flow of energy to a 'two-way' flow, communication has never been more critical. International standards such as IEC 61850, IEC62351, and IEC 62443 provide guidelines for effective communication among network and power systems. There is an opportunity for Australia to adopt these standards.

Subtopics:

- Network Communication
- Power System Control
- Smart Grids
- Metering

Risk Management Techniques

The cyber security standards developed by ISO/IEC JTC 1 provide a robust toolkit for information security management. The key challenge is to leverage these techniques

to maintain the availability and safety of control systems. There are a number of international and Australian adopted standards in this area, however the key is to integrate security management technologies into critical infrastructure design from the outset as well as provide mechanisms for retrospective upgrades on existing infrastructure.

Subtopics:

- Cyber Security
- Information Security
- Physical Security

Terminology and Data Management

An understanding of how data is generated and used is vital as the power grid becomes smarter. IEC 61850 sets out core data semantics for the power system, however the data generated from networking devices such as meters and sensors can be transformed into analytics that impact strategic decision making. Standards relating to data management in the energy sector are limited and there is a need to collaborate with other sectors to develop and/or adopt standards in this area.

Subtopics:

- Vocabulary/semantics
- Frameworks

Privacy

As the grid transforms, it is important that exposure to privacy and personal data breaches are mitigated. Standards offer an avenue to provide guidelines on how to assist in meeting customer and community expectations pertaining to privacy.

The five key thematic areas for grid cyber security highlighted above were also covered by Energy Networks Australia's 2017 report 'Cyber Security and Energy Networks' where they identified four broad dimensions of cyber security for the energy system. These include:

- The grid systems and components relied on by energy networks, including technology providers, individual components or systems they procure;
- The control systems used to monitor and control the network to support energy flows safely and reliably;
- The access to data which safeguards privacy and commercial confidentiality; and
- The diverse and growing distributed resources which increasingly form a core part of the energy system.

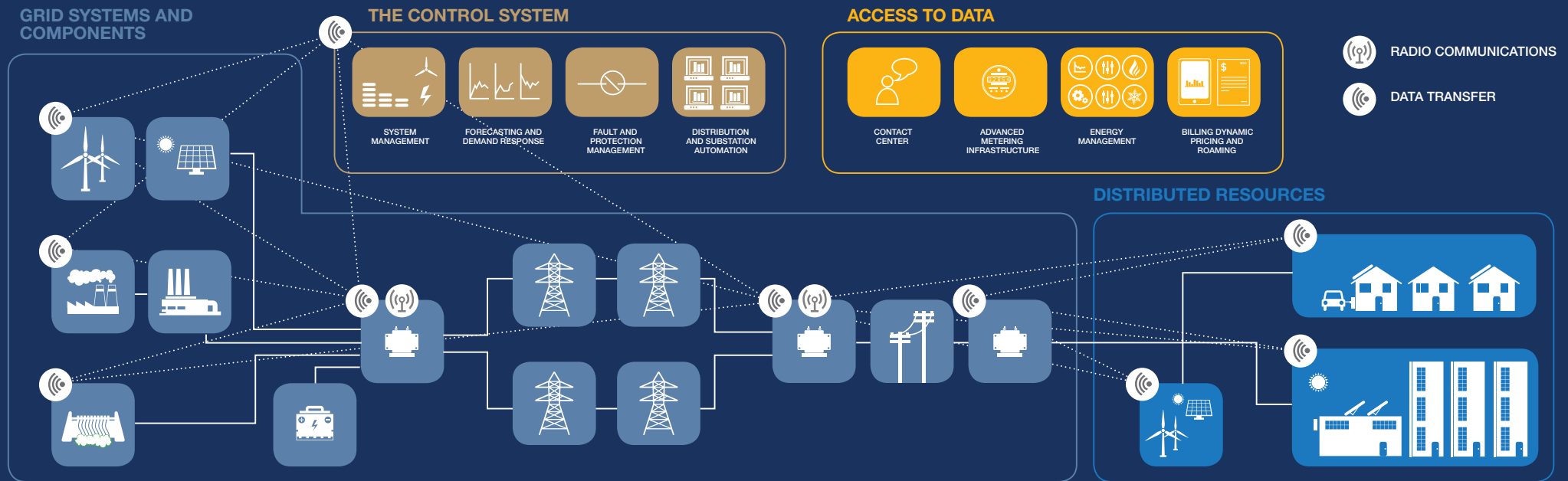


Figure 1 Cyber Security and Energy Networks

Consultation Approach

The Roadmap exercise included consultations in major capital cities of Perth, Adelaide, Brisbane, Sydney, Melbourne and Canberra and the development of a consultation discussion paper which was published on Tuesday 9 October 2018. In addition, a National Forum on Grid Cyber Security was held on Thursday 18 October 2018. All phases of the consultation sought to elicit from government, industry, consumer groups and other interested parties, their perspective on the standardisation needs outlined by the topic areas.

National Consultation and National Forum

Discussion Paper

The discussion paper was designed to serve three key purposes:

1. Seek feedback on the current state of standards and committees in each of the topic areas;
2. Understand if there is consensus for any urgent work to be undertaken; and
3. Coordinate development of a roadmap for future standards development and associated actions over the coming years, and time frames for those activities.

Stakeholders were requested to provide their input and perspectives on standardisation of cyber security and the grid.

The discussion paper ([download PDF here](#)) encouraged responses to a series of questions by presenting each topic area with its associated sub-topics.

The discussion paper included a table of supplementary information for each topic area suggesting the relevant Australian committees (and their activity level) and standards in those topic/functional areas, and also highlighted the relevant IEC/ISO committees (and whether Australia participated/observed), and related standards.

Summary of National Consultation

At the National Forum on Grid Cyber Security stakeholders (see Appendix A) identified five key focus areas which were discussed. These include risk management, infrastructure resilience, terminology and data management, networks and power systems communications and privacy. In addition stakeholders raised the need to consider hardware, software and supply chain standards to support the future of distributed energy networks in Australia.

Stakeholders agree that internationally aligned cyber security standards for the energy grid are of crucial importance not only for energy companies but also consumers, retailers and the broader economy in Australia. Internationally aligned standards support interoperability, communication and trust of existing energy networks and the growing role of distributed electricity networks. International standards bring technological, economic and societal benefits to Australia.

Trust was a consistent theme from the consultations. Stakeholders regularly voiced support for a descriptive risk based approach to cyber security rather than a prescriptive standards approach. This is particularly important as the distributed energy system is changing with the emergence of prosumers and new players in an increasingly decentralised system.

Key areas of current vulnerability for the grid include structural change of the grid with greater interconnectivity, building management systems (BMS), IoT, increasing blurring between Operational Technology (OT) and Information Technology (IT) systems, artificial intelligence (AI) and the rise of cybercrime as a business.

In addition, stakeholders also identified that good engineering practices such as up to date registers, data flow diagrams, version management procedures, auditable logging for all actions support cyber security resilience and may be able to be automated as part of a well-implemented device management system.

The importance of interoperable internationally aligned standards was supported by stakeholders across government, industry and academia. In addition, there is a need to focus on the training and development of internal and external staff and stakeholders to ensure proper awareness and that cyber protocols are followed. These include human resource management techniques, authentication protections, the alignment of internal Cyber Security Capability Maturity Models (C2M2) and incentive structures to mitigate cyber security threats.

The majority of Australian power utilities employ SCADA systems that use the IEEE Standard 1815 (DNP3) protocol for field communication. The deployment lifetime of control system equipment is often in the 10 to 20 year range for the energy transmission sector. A key point raised by stakeholders was that even if new standards for all these management functions were available today, it would be many years before equipment supporting them would be deployed and some small simple devices such as IIoT devices may never support such complex features.

Apart from the SCADA system itself, the remote electrical stations (generators, substations and loads) are increasingly deploying Ethernet based technologies at the sensor, protection, controller and metering device level, notably increasingly based on IEC 61850 released in 2004. These Intelligent Electronic Devices (IEDs), and their configurations, are critical to the real time operation of the power system. The integration of the SCADA and IED communication systems is significantly expanding the size and number of critical cyber assets within the power sector beyond just the considerations for head office and SCADA systems.

Stakeholders also identified a number of related standardisation areas that support grid cyber security. These include workforce screening, fraud and corruption control, physical protective security treatment for buildings and workforce data quality. Given that grey hat 'insiders' account for around 60 percent of all cyber-attacks, stakeholders discussed the possibilities to address this issue through standardisation¹. In particular, an update to AS 4811:2006 'Employment Screening' may help to address this through a risk-based, all-hazards workplace decision making approach. Stakeholders agreed that currently, there is not a consistent industry approach to workforce screening presenting possible vulnerabilities in regards to cyber security.

National Forum

On 18 October 2018, Standards Australia hosted the Grid Cyber Security National Forum (Forum) at Standards Australia's Sydney office. This was an opportunity for industry, government, regulators, academics, consumers and others to come together, to express their views and help prioritise and identify future standardisation activities.

The Forum was made up of three sections. The first section provided context as to the genesis of the initiative and why ENA had partnered with Standards Australia. Dr Bronwyn Evans, CEO, Standards Australia and Dr Stuart Johnston, General Manager,

¹ IBM X-Force Research, 2016 Cyber Security Intelligence Index

Energy Networks Australia formally opened the Forum. The second section included three keynote speakers providing an overview of the evolving distributed electricity system and cyber security. Mr Ryan Wavish, CEO, Marchment Hill Consulting presented an overview of the coming changes to the distributed energy industry across Australia. Mr Andrew Kiley, Assistant Secretary, Department of Home Affairs highlighted to the Forum Australia's whole of government engagement and focus on cyber security. Dr Mike Johnstone, Associate Professor, Edith Cowan University presented on the future areas of cyber security research and current international cyber standards.

The third section of the Forum included stakeholder breakout discussions and a prioritisation session.

More than 50 participants registered for the Forum with stakeholders representing market and network operators, government, consumers, academics, industry consultants, regulators and other specific industry associations. The Forum represented perhaps the first time so many stakeholders from diverse backgrounds came together to discuss the future of grid cyber security and the role of standards.

National Forum Response

During the Forum proceedings, the key themes raised in the discussion paper and responses re-appeared. The need for interoperable systems which maintain reliability of supply, security across OT and IT systems was a key focus for stakeholders. Stakeholders identified the need for internationally aligned standards to support these goals. Stakeholders noted that current industry practice was to apply different national, regional and international standards to support their businesses and operations. This highlighted the need for international standards setting bodies to ensure greater coordination and participation across thematic areas to minimise the risk of overlapping future cyber security standards leading to the balkanisation of international standards. Duplication of international standards may increase compliance costs for the Australian energy transmission industry and reduce interoperability between networks.

The following items were discussed:

Distributed Energy Coordination

Distributed energy coordination and the encouragement of open standards and operability were raised at various points during the Forum. Stakeholders highlighted that as the grid transforms, standards should not be prescriptive to the point of unintentionally stifling the development of new markets and technologies but rather be performance based, focussing on outcomes rather than a step-by-step "deemed to comply" solutions. This is critical to allowing the development and integration of new sources of distributed energy into the grid network. Stakeholders also highlighted the importance of internationally aligned standards with Australian participation to ensure standards developed at the IEC, ISO and other bodies suit Australian market needs.

Infrastructure Resilience

Stakeholders including representatives from the Department of Home Affairs Critical Infrastructure Centre identified energy networks as a key part of the Australian economy. As the economy continues to evolve with greater use of digital services and devices, reliable electricity supply is essential to the broader economy. Examples provided by speakers such as recent attacks on the Ukrainian and US power grids demonstrates the rise of non-state and state actors and the importance of ensuring the energy network continues to build cyber resilience. Malicious intent and greater access through a distributed network raises the risks for cyber intrusions without appropriate

mitigation strategies. Therefore infrastructure resilience was identified as a key area of standardisation requiring urgent attention by stakeholders.

Network and Power Systems Communications

As the energy grid is transforming to include decentralised electricity sources and the advent of prosumers, network and power systems communications are critical to enabling this transformation. International standardisation in this area was identified as a key focus by stakeholders. A number of international standards committees were identified for future Australian participation. In addition, stakeholders called for greater coordination and cooperation of Standards Australia's committees to help address cyber security from a whole of industry perspective. In particular, stakeholders called for the participation on key international committees at the ISO and IEC. These are namely ISO TC 184 Automation Systems and Integration and IEC TC 72 Automatic Electrical Control. Currently Australia is not an observer or participating member of these committees.

Terminology and Data Management

The transformation of the energy grid and the application of information and communication technologies such as smart meters, IIoT, and artificial intelligence require consistent and consensus driven terminology and data management practices. This will support interoperability and trust especially for consumers and prosumers who may have a limited awareness and application of terminology and data management standardisation approaches. Stakeholders identified a number of international standards such as ISO 27000 Series of Information Security Management as a trusted and useful starting point for the industry. Stakeholders however indicated that it would be useful for the energy industry to learn and apply best practice from other sectors of the Australian economy such as in financial services.

Risk Management

Stakeholders raised the importance of risk management techniques and appropriate internationally aligned standards and frameworks to help address the challenges of cyber intrusions. According to stakeholders one of the greatest risks is the communication of how to approach risks. Although industry has historically applied parts of international standards there was now a view that industry was moving away from standalone standards towards more holistic management frameworks such as through NIST in the USA. The rationale from industry for applying the NIST Cyber Security Framework in Australia was that it can be easily understood and implemented by industry as relevant. The framework includes five clear categories for performance to be reported. These include, identify, protect, detect, respond and recover.

Stakeholders agreed that a consistent approach to measure risk is essential for building trust and supporting grid cyber security resilience. Standard needs to cover capability to respond to risk, managing through to addressing risk. Given the critical nature of the energy grid and electricity networks it is important that appropriate risk management frameworks continue to evolve as the industry evolves. It is important that suitable scope is built into risk management frameworks and not just to include a 'protect' element. In addition, a number of stakeholders raised the concept of applying learnings from financial services principles especially in regards to counter fraud controls and counter-terror mitigation.

Stakeholders also identified a number of related standardisation areas that support grid cyber security and risk management. These include workforce screening, fraud and corruption control, physical protective security treatment for buildings and workforce data quality.

Privacy

Privacy was identified by stakeholders as a key consideration facing the industry in dealing with grid cyber security. In addition to national legislation such as the Privacy Act 1988 in Australia many stakeholders indicated that internationally they face a growing privacy regulatory landscape. The increasingly application of IIoT and other information and communications technology in the energy grid especially in distributed electricity elements raises the level of data and possible personal information generated and collected. This has escalated the potential financial and reputational costs of cyber intrusions. Stakeholders raised a general concern in regards to the increasing amounts of information available to business through smart devices, IoT and remote access.

International Harmonisation

Consensus was reached by stakeholders for the importance of ensuring Australian standards are harmonised with international standards. Stakeholders unanimously agreed that one of the key actions to facilitate grid cyber security in Australia is international engagement and harmonisation. Participants agreed that generally Australian mirror committees to the ISO and IEC were the appropriate mechanism for engagement.

Action Plan

In considering the responses received during the discussion paper consultation, national forum and national consultations, the priorities identified are collated into a list of actions.

The Roadmap identified the following items of particular importance:

- Recommendation for the development of standards and documents to support grid cyber security in Australia including workforce screening
- Submit proposals for 'P' membership of ISO TC 184 Automation systems and integration, IEC TC 72 Automatic Electrical Control and IEC SyC, Smart Energy
- Proposal for a new Australian mirror committee to IEC 1 Terminology

A recommendation for the development of standards and documents to support grid cyber security in Australia

AS 4811 – Workforce Screening (previously known as Employment Screening)

The key objective of this revision will move the standard from a process approach and establish a risk-based, all-hazards workplace decision-making approach. It looks to implement a whole-of-person lifecycle monitoring approach, thus enabling organisations to be more responsible for their own and their workforce's needs according to changing risk context. Maintaining screening and monitoring processes for the duration of engagement and, where possible or where necessary, beyond is important. Positive and

informed communications with the workforce and other stakeholders has been identified as a critical new area needed within the standard to support more timely identification of continuous learning and improvement.

AS 8001 – Fraud and Corruption Control

There have been significant developments within the discipline of fraud and corruption control that should be taken into account in the revision of the Standard. One of the key developments is the recognition that employee engagement can play a significant role in controlling fraud and corruption. In addition, issues such as supply chain management, outsourcing, cybercrime, identity theft, artificial intelligence, applied psychology, models of decision-making, assurance mapping, probity auditing, social media, mobility between private and public sectors and technological change have significantly changed in nature since the Standard was last issued. In the last ten years, there have also been changes in the field of compliance and governance that impact on fraud and corruption control. Internationally, anti-corruption requirements and guidelines bring increased attention to assurance frameworks and measures. They emphasise the importance of controls being more than “paper” measures that look good but are not effectively applied.

HB-188 - Physical Protective Security Treatment for Buildings Handbook

In anticipation of terrorist and other malicious physical threats, owners and operators of major Australian buildings bear responsibility for managing a physical risk to their assets and operations. This new Handbook will crystallise the various publications of existing guidance and support proactive risk management of large-scale infrastructure. This Handbook will compile existing standards, ISO documents, national Government advice and industry expertise into one easily accessible document and provide an opportunity for improved assessment, prevention and treatment methodologies.

Workforce Data Quality (new standard)

Standards Australia Committee MB-009 Human Resources and Employment, is focusing on the development of Human Resource (HR) Standards to support all sectors of Australian Industry. There are numerous metrics described in a range of international Standards and it has been established that there is a need to develop a standard that outlines the quality of the data being used within these metrics. Currently, the primary role of existing standards focuses on the reporting processes within HR functions rather than the quality and consistency of data that they collect. Much has been written about the overall impact of poor data quality on businesses with it cited as a primary reason for 40% of all business initiatives failing to achieve their targeted benefits and effecting overall labour productivity by as much as a 20%²

A range of stakeholders have indicated that these four standards are intrinsically linked from a security, risk, resilience and governance perspective as an organisation's assessment of staff and the individual levels of risk they post are only as good as the data you collect and maintain.

2 Measuring the Business Value of Data Quality, Ted Friedman, Michael Smith, Gartner, 2011

A recommendation for Australian participation in the following international standards committees (see appendix B for further information)

- ISO TC 184 Automation systems and integration
- IEC TC 72 Automatic Electrical Control
- IEC SyC Smart Energy
- IEC TC 1 Terminology

A recommendation for the review of membership and terms of reference for the following the Australian Technical Committees (see appendix B for further information)

- EL-064 Decentralised electrical energy and grid integration of renewable energy systems (mirror committee to TC 8C)
- IT-012 Information Security, Systems and Identification Technology (mirror committee to ISO/JTC 1 SC 27 Information Technology Security Techniques) be reconstituted to include distributed energy industry representatives
- MB-025 Security mirror committee of ISO TC 292 Security and Resilience to include distributed energy industry representatives
- OB-007 Risk Management mirror committee of ISO TC 262 Risk Management to include distributed energy industry representatives
- Merge EL-050 Power Systems control and communication as mirror to IEC TC 57 Power systems management and associated information exchange with the Australian EL-62 Smart Grids committee (mirror committee to IEC PC 118 which Australia is a 'P' member)
- Propose a data meeting under JTC SAC and IEC National Committee to coordinate standardisation efforts related to data frameworks and data privacy

Conclusion

The report summarises the actions undertaken in the Roadmap, and is an informative tool for stakeholders that recognises the importance of allowing the development of markets and business while providing support through future standards development. The agenda of Standards Australia and the program of work it undertakes is driven by stakeholders, including industry organisations, network operators and other market participants and indeed regulatory agencies and relevant government departments. It is therefore critical that the recommendations of the report be driven by key industry and government stakeholders so that standardisation gaps can be closed.

The report has identified the need to engage internationally, specifically with a number of Systems Committees and Technical Committees at the International Electrotechnical Commission (IEC). Policies that drive international standards participation will ensure that Australia's perspectives are incorporated at this level, facilitating the potential national uptake of standards produced by these groups.

These groups have been identified by stakeholders as key resources supporting cyber resilience of the grid. Participating at international standardisation efforts has been identified as critical to ensure that Australian stakeholders are standards makers and not just standards consumers. In many areas Australia punches above its weight such as blockchain, and IT governance. Through collaboration of government, industry and relevant stakeholders, Australia can continue this trend by taking advantage of the opportunities identified in this report.

The report includes input from stakeholders and supports a recommendation of the Network Transformation Roadmap undertaken by ENA and the CSIRO.

Appendix A: Industry Workshop

This appendix provides a list of organisations which registered to attend the National Forum

Ausgrid	Power and Water Northern Territory
Ausnet Services	Powercor Australia
Australian Energy Market Operator	Powerlink Queensland
Australian Industry Group	Queensland University of Technology
Australia Chamber of Commerce and Industry	Tasnetworks
Australian Energy Market Operator	Transgrid
Australian Industry Group	United Energy
Australian Information Security Association	University of New South Wales
BRM Holdich	University of Melbourne
Consumers Federation of Australia	Victoria University
Deakin University	Woolworths
Department of Foreign Affairs and Trade	Stakeholders part of national consultations
Department of Home Affairs	Blue IoT
DNV GL	Endeavour Energy
Edith Cowan University	Premier and Cabinet, Government of South Australia
Energy Networks Australia	Premier and Cabinet, Government of Western Australia
Engineers Australia	Murdoch University
GHD	University of Queensland
Horizon Power	Monash University
Institute of Instrumentation, Control & Automation Aust Inc	RMIT
Jemena	Rod Hughes Consulting
Macquarie University	Western Power
Marchmont Hill Consulting	Santos
Origin Energy	Subnet Solutions Inc

Appendix B: Action Plan Committees

Topics/subtopic area	Actions	By Whom	Milestones	Expected Implementation Period
Network and Power Systems Communications	Consider merging EL-050 Power Systems control and communication as mirror to IEC TC 57 Power systems management and associated information exchange with the Australian EL-62 Smart Grids committee (mirror committee to IEC PC 118 which Australia is a 'P' member)	Standards Australia working with relevant stakeholders	<ul style="list-style-type: none"> Identify champions and email stakeholders (January 2019) Reconstitute mirror committee (April 2019) Convene first meeting and assess work program (May 2019) Convene a joint meeting of EL-50 and EL-62 to consider the value in merging these committees (June 2019) 	Mid 2019
	Setup Australian mirror committee to ISO TC 184 Automation systems and integration and develop a 'Case for International Participation'	Stakeholders – potentially network operators, government or industry participants	<ul style="list-style-type: none"> Identify champion and email stakeholders (February 2019) Assess proposals for mirroring activities (March 2019) Constitute mirror committee (June 2019) Convene first meeting and assess work program (July 2019) 	Mid 2019
	Setup Australian mirror committee to IEC TC 72 Automatic Electrical Control and develop a 'Case for International Participation'	Stakeholders – potentially network operators, government or industry participants	<ul style="list-style-type: none"> Identify champion and email stakeholders (February 2019) Assess proposals for mirroring activities (March 2019) Constitute mirror committee (June 2019) Convene first meeting and assess work program (July 2019) 	Mid 2019

Topics/subtopic area	Actions	By Whom	Milestones	Expected Implementation Period
Infrastructure Resilience	Review the constitution and TOR of EL-064 Decentralised electrical energy and grid integration of renewable energy systems (mirror committee to TC 8C Decentralized Electrical Energy Systems which Australia has recently become a 'P' member	Standards Australia working with relevant stakeholders	<ul style="list-style-type: none"> Identify champions and email stakeholders (March 2019) Consider Reconstitute mirror committee (April 2019) Convene first meeting and assess work program (July 2019) 	Mid 2019
	Setup Australian mirror committee to IEC SyC Smart Energy and develop a 'Case for International Participation'	Stakeholders with the support of Standards Australia – potentially network operators	<ul style="list-style-type: none"> Identify champion and email stakeholders (January 2019) Assess proposals for mirroring activities (April 2019) Constitute mirror committee (June 2019) Convene first meeting and assess work program (July 2019) 	Mid 2019
Terminology and Data Management	Setup Australian mirror committee to IEC TC 1 Terminology and develop a 'Case for International Participation'	Stakeholders – potentially network operators, retailers, or regulators/ government	<ul style="list-style-type: none"> Identify champion and email stakeholders (February 2019) Assess proposals for mirroring activities (March 2019) Constitute mirror committee (June 2019) Convene first meeting and assess work program (July 2019) 	Mid 2019

Topics/subtopic area	Actions	By Whom	Milestones	Expected Implementation Period
Privacy	Convene a data meeting under JTC SAC and IEC National Committee to coordinate standardisation efforts related to data frameworks and data privacy	Standards Australia	<ul style="list-style-type: none"> Raise at next IEC National Committee meeting and JTC 1 SAC meeting (July 2019) 	Mid 2019
	Amend constitution of IT-012 Information Security, Systems and Identification Technology (mirror committee to ISO/JTC 1 SC 27 Information Technology Security Techniques) be reconstituted to include distributed energy industry representatives	Standards Australia	<ul style="list-style-type: none"> Identify champion and email relevant stakeholders (January 2019) Re-constitute mirror committee (May 2019) 	Mid 2019
Risk Management Techniques	Consider amending constitution of MB-025 Security mirror committee of ISO TC 292 Security and Resilience to include distributed energy industry representatives	Standards Australia	<ul style="list-style-type: none"> Identify champion and email relevant stakeholders (January 2019) Re-constitute mirror committee (May 2019) 	Mid 2019
	Consider amending constitution of OB-007 Risk Management mirror committee of ISO TC 262 Risk Management to include distributed energy industry representatives	Standards Australia	<ul style="list-style-type: none"> Identify champion and email relevant stakeholders (January 2019) Re-constitute mirror committee (May 2019) 	Mid 2019

Appendix C: Standards Overview

Infrastructure Resilience

Sub Topics	<ul style="list-style-type: none"> • Energy Supply (Generation, Transmission, Distribution) • Microgrids • Asset and Facilities Management 	
Committees operating in this functional area	Standards Australia Committees	International Committees
	EL-034 Power Quality (A)	IEC TC 8 System aspects of electrical energy supply (P)
	EL-064 Smart Grids (A)	SC 8B Decentralised Electrical Energy Systems (O)
	EL-042 Renewable Energy Power Supply Systems & Equipment (A)	IEC TC 82 Solar photovoltaic energy (P)
	EL-052 Electrical Energy Networks, Construction and Operation (A)	
	EL-001-24 Generating Sets	
	EN-001 Energy Auditing (A)	ISO TC 301 Energy management and energy saving (P)
	EN-004 Energy Network Management and Safety Systems (I)	
	FP-017 Emergency Management Procedures (A)	
	MB-025 Security (A)	<ul style="list-style-type: none"> • ISO TC 292 Security and Resilience (P)
	MB-019 Asset Management (A)	<ul style="list-style-type: none"> • ISO TC 251 Asset management (P)
	MB-022 Facilities Management (A)	<ul style="list-style-type: none"> • ISO TC 267 Facilities Management (P)
Australian Standards in this functional area	<ul style="list-style-type: none"> • AS/NZS 3010:2005 Generating Sets • AS/NZS 4509 series Stand-alone power systems • AS/NZS 4777 series Grid connection of energy systems via inverters • AS/NZS 5033:2014 Installation and safety requirements for photovoltaic arrays • AS 3745-2010 Planning for emergencies in facilities • AS 5577:2013 Electricity network safety management systems • AS ISO 55000:2014 Asset management - Overview, principles and terminology • AS ISO 55001:2014 Asset management - Management systems – Requirements • AS ISO 55002:2014 Asset management - Management systems -- Guidelines for the application of ISO 55001 • AS ISO 22301:2017 — Societal security - Business continuity management systems – Requirements • AS ISO 22313:2017 — Societal security - Business continuity management systems – Guidance • SA TS ISO 22317:2017 — Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA) 	
IEC/ISO Standards in this functional area	<ul style="list-style-type: none"> • IEC 60255 Measuring relays and protection equipment • IEC/TR 62511 ed1.0 — Guidelines for the design of interconnected power systems • IEC/TS 62898-1 Guidelines for general planning and design of microgrids • IEC/TS 62898-2 Technical Requirements for Operation and Control of microgrids • IEC/TS 62786 Distributed Energy Resources Interconnection with the Grid • ISO 14084 series Process diagrams for power plants Requirements • ISO 22316:2017 — Security and resilience — Organizational resilience — Principles and attributes • ISO/TS 22318:2015 — Societal security — Business continuity management systems — Guidelines for supply chain continuity • ISO 28000:2007 Specification for security management systems for the supply chain • ISO 50001:2011 — Energy management systems — Requirements with guidance for use 	

Network and Power Systems Communications

Sub Topics	<ul style="list-style-type: none"> • Network Communication • Power System Control • Smart Grids • Metering 	
Committees operating in this functional area	Standards Australia Committees	International Committees
	EL-011 Electricity Metering Equipment (A)	IEC TC 13 Electrical Energy Management and Control (P)
	EL-050 Power System Control and Communication (A)	IEC TC 57 Power systems management and associated information exchange (P)
	EL-052 Electrical Energy Networks, Construction and Operation (A)	
	EN-004 Energy Network Management and Safety Systems (I)	
	EL-062 Smart Grids (A)	IEC PC 118 Smart grid user interface (P)
		ISO TC 184 Automation systems and integration
		IEC TC 72 Automatic electrical controls
	IT-006 Industrial Process Measurement, Control and Automation (A)	IEC TC 65 Industrial-process measurement and control (P)
Australian Standards in this functional area	<ul style="list-style-type: none"> • AS 5577-2013 – Electricity network safety management systems • AS 61508 series Functional safety of electrical/electronic/programmable electronic safety related systems • AS 1284 series Electricity metering • AS 62052 series Electricity metering equipment (AC) - General requirements • AS 62053 series Electricity metering equipment (AC) - Particular requirements • AS 62054 series Electricity metering equipment (AC) - Tariff and load control • AS 62056 series Electricity metering - Data exchange for meter reading, tariff and load Control • AS ISO 14649.1:2004 Industrial automation systems and integration 	
IEC/ISO Standards in this functional area	<ul style="list-style-type: none"> • IEC 61069 series Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment • IEC 61158 series Industrial communications networks - Fieldbus specifications • IEC 61334 series Distribution automation using distribution line carrier systems • IEC 61850 series Communication networks and systems for power utility automation • IEC 61968 series Application integration at electric utilities - System interfaces for distribution management • IEC 61970 series Energy management system application program interface • IEC 62325 series Framework for energy market communications • IEC 62351 series Power systems management and associated information exchange – Data and communications security • IEC 62361 series Power systems management and associated information exchange - Interoperability in the long term • IEC 62443 series Industrial communication networks - Network and system security • IEC 62746 series Systems interface between customer energy management system and the power management system • ISO 16484 series Building automation and control systems • ISO/IEC 14908 series Information technology - Control network protocol 	

Sub Topics	<ul style="list-style-type: none"> • Cyber Security • Information security • Physical Security 	
Committees operating in this functional area	Standards Australia Committees	International Committees
	IT-012 Information Systems, Security and Identification Technology (A)	ISO/IEC JTC1 SC27 Information Technology Security Techniques (P)
	MB-025 Security (A)	ISO TC 292 Security and Resilience (P)
	OB-007 Risk Management (A)	ISO TC 262 Risk Management (P)
Australian Standards in this functional area	<ul style="list-style-type: none"> • AS ISO/IEC 27001:2015 Information technology - Security techniques - Information security management systems • AS ISO/IEC 27002:2015 – Information technology - Security techniques - Code of practice for information security controls • AS ISO/IEC 27004:2018 – Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation • AS ISO/IEC 27035.1:2017. – Information technology—Security techniques—Information security incident management. Part 1: Principles of incident management • AS ISO/IEC 27035.2:2017 – Information technology—Security techniques—Information security incident management, Part 2: Guidelines to plan and prepare for incident response • HB 167:2006 Security risk management • AS 1725.1-2010 Chain link fabric fencing - Security fences and gates - General requirements • AS/NZS 3016:2002 Electrical installations - Electric security fences • AS/NZS 4421:2011 Guard and patrol security services • AS/NZS ISO 31000-2009 – Risk management - Principles and guidelines 	
IEC/ISO Standards in this functional area	<ul style="list-style-type: none"> • IEC 62351 series Power systems management and associated information exchange - Data and communications security • ISO/IEC 27000 series Information technology - Security techniques - Information security management systems • ISO/IEC 27019:2017 Information technology - Security techniques - Information security • ISO 18788:2015 Management system for private security operations - Requirements with guidance for use • ISO 31000: 2018 Risk management - Guidelines 	

Terminology and Data Management

Sub Topics	<ul style="list-style-type: none"> • Vocabulary • Frameworks 	
Committees operating in this functional area	Standards Australia Committees	International Committees
	EL-062 Smart Grids (A)	IEC PC 118 Smart grid user interface (P)
	JTC 1 SAC (Strategic Advisory Committee) (A)	ISO/IEC JTC 1 Information Technology (P)
	IT-012 Information Systems, Security and Identification Technology (A)	ISO/IEC JTC1 SC27 Information Technology Security Techniques (P)
		ISO/IEC JTC1 SC32 Data management and interchange
	MB-025 Security (A)	ISO TC 292 Security and Resilience (P)
Australian Standards in this functional area	<ul style="list-style-type: none"> • AS 5711:2013 Smart grid vocabulary • ISO 22300:2018 — Security and resilience — Vocabulary 	
IEC/ISO Standards in this functional area	<ul style="list-style-type: none"> • IEC 62939-3 Smart grid user interface - Part 3: Energy interoperation services 	

Privacy

Committees operating in this functional area	Standards Australia Committees	International Committees
	IT-012 Information Systems, Security and Identification Technology (P)	ISO/IEC JTC1 SC27 Information Technology Security Techniques
IEC/ISO Standards in this functional area	<ul style="list-style-type: none"> • ISO/IEC 27018:2014 Information technology - Security techniques - Code of practice for protection of personally identified information (PII) in public clouds acting as PII processors • ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework • ISO/IEC 29100:2011/Amd.1:2018 — Information technology — Security techniques — Privacy framework AMENDMENT 1: Clarifications 	