1 March 2024

24-28 Campbell St
Sydney NSW 2000
All mail to
GPO Box 4009
Sydney NSW 2001
T +61 2 13 13 65
ausgrid.com.au

Cyber Security Expert Advisory Board
Andrew Penn AO (Chair)
Air Marshall (ret'd) Mel Hupfeld AO DSC
Rachael Falk
Submission made by webform

Ausgrid response to the 2023-30 Australian Cyber Security Strategy: Legislative Reform Consultation Paper

Dear Mr Penn, Air Marshall Hupfeld and Ms Falk,

We welcome the opportunity to respond to the Cyber Security Expert Advisory Board's (**the Board**) *2023-30 Australian Cyber Security Strategy: Legislative Reform Consultation Paper* (**Consultation Paper**).

Ausgrid operates a shared electricity network that powers the homes and businesses of more than 4 million Australians living and working in an area that covers over 22,000 square kilometres from the Sydney CBD to the Upper Hunter.

As the most populous network area and financial capital of Australia, over 20 per cent of Australia's GDP is generated within our network area. We supply energy to 105 hospitals, Australia's only radiopharmaceuticals production facility, 4 of the world's top 200 ranking universities, 3 major ports and 37% of Australia's financial services industry. This means that a cyber-attack on our network, even for a few hours, would severely disrupt lives and livelihoods. In the worst possible case, the economic impact from a complete shutdown of our infrastructure may be as high as $120 million per hour or over $2.9 billion per day.

We support the Board's ambitions for Australia to become the most cyber secure nation in the world by 2030 and broadly supports the Consultation Paper.

We have included our response to the Consultation Paper's questions in **Attachment A**. However, we note that the extent of Ausgrid's ability to improve cyber security resilience on our network is dependent on cyber security program approval from the Australian Energy Regulator in April 2024, which will provide Ausgrid with funding to mitigate cyber risks from 1 July 2024 to 30 June 2029. We note that where expenditure is subject to approval by a regulator, it would assist both the business and the regulator for the appropriate security protocol level to be defined in the SOCI Act. This would avoid any subjectivity in relation to risk assessments about the appropriate security protocol level the business should attain.

We welcome the opportunity to discuss any aspect of our submission with you. Please contact Naomi Wynn, Regulatory Policy Manager, [redacted].

Regards,

[redacted]

Murray Chandler
Head of Network Strategy & Future Grid

Attachment A – Ausgrid response to key questions

#	Question	Ausgrid's response
Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices		
1	Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?	Ausgrid recommends that the whole supply chain should have positive obligations to comply with a proposed mandatory cyber security standard. This should include component manufacturers, compilers and product vendors. These obligations should gradually increase to ensure continuous improvement over a defined timeline, without imposing an extensive regulatory burden.
2	Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?	Ausgrid supports these first three principles as an appropriate minimum baseline for consumer-grade IOT devices sold in Australia.
3	What alternative standard, if any, should the Government consider?	Ausgrid recommends that the Government consider including other suitable international standards/guidance including: • The National Institute of Standards and Technology (**NIST**) Cybersecurity for Internet of Things (**IOT**) Program; • The Institute of Electrical and Electronics Engineers (**IEEE**) IOT Security of Best Practices (February 2017); and • The International Organisation for Standardisation (**ISO**) ISO/IEC 27400:2022 - IoT security and privacy – Guidelines.
4	Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?	Ausgrid supports a broad definition of smart devices that are subject to an Australian mandatory standard, drawing on the PTSI Act in the UK and other relevant international approaches for guidance. For example, it should include customer energy resources such as solar inverters and batteries. The definition should also include consideration of the context of where the device is to be used and use of device's context. For example, a specific context that arises with electricity networks, are smart devices that are 'network connectable' but only utilised on the electricity network's owned and operated secure, non-public internet facing communications network.

5	What types of smart devices should not be covered by a mandatory cyber security standard?	Ausgrid recommends that industrial internet of things (**IIOT**) should have mandatory cyber security standards. We note that these standards will be different to IOT due to the context of where and how the device is being used and what function it supports. A risk-based evaluation should apply when determining which IOT to define to ensure that the framework does not become too cumbersome. This should include consideration of what is and is not a 'technology', as in some circumstances it can be an electronic device, network or connected device. For example, there should be an exemption process for smart devices that do not meet mandatory standards, but that can demonstrate the application of a detailed risk assessment process aligned to the CIRMP to warrant using that smart device by a licensed utility (i.e. not the general businesses and consumers). These exemptions could be provided to DOHA as part of regular risk management reporting requirements. This exemption process is necessary to balance the maturity and cost of IOT smart devices. Factors in the risk assessment could include demonstrating how the non-compliant smart device: • Is limited to a trial or specific stand-alone project; • Is limited to isolated systems; • Provides increased efficiency; • Is more cost efficient; • Does not impact critical asset processes or function; or • Is only needed until the market for its use matures and delays would impact a utility adopting modern technologies in a timely manner.
6	What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?	Ausgrid recommends a 5-year timeframe is sufficient for industry to adjust to new cyber security requirements for smart devices. This is a reasonable timeframe given the life cycle for these types of technologies and devices.
7	Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?	Ausgrid considers that the Regulatory Powers Act may be a suitable baseline framework depending upon the powers that are given to the relevant regulatory body and the circumstances in which those powers are exercised. However, it is difficult to say at this early stage whether this is suitable given those matters are still to be settled. In any event, Government should look to give the relevant regulatory body the minimum powers necessary to achieve its desired outcomes and functions.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses		
8	What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?	Ausgrid recommends that the Government apply the principle of who, what, when, where, why and how as the threshold for mandatory reporting information. We also recommend that the Government ensure that these reporting obligations are streamlined into one process and through one entity so that entities know the reporting steps in an incident.
9	What additional mandatory information should be reported if a payment is made?	See response to question 8. The 'What' question should include confidential information about payments.
10	What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?	The scope of ransomware reporting should be proportionate to the impact to the organisation's revenue, staff and customers. See response to question 11 below.
11	Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?	Ausgrid supports the $10 million per year threshold for mandatory reporting. However Ausgrid sees merit in lower threshold voluntary reporting so that the Government can release case studies and alerts about incidents that impact smaller entities.
12	What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?	Ausgrid recommends that entities should be required to provide a preliminary report within 72 hours, with more detail following investigation. We do not recommend a timeframe for detailed reporting as it will depend on the complexity of the incident and will need to be agreed upon between relevant parties based on the circumstances.
13	To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?	Ausgrid strongly supports applying the no-fault and no liability principles to encourage reporting.

14	How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?	Ausgrid suggests that the Government ensure that no-fault and no-liability principles can be balanced with public expectations that businesses take accountability for their cyber security by anonymising the public reporting and ring-fencing incidents from compliance and risk management reporting.
		
		The Government can also categorise incidents to determine the reasonableness of response depending on:
		• The incident's size;
		• The entity's size in terms of:
		  ○ Number of customers impacted, and
		  ○ Revenue; and
		• The aggregate ransom or dollar-impact to customers of the incident in aggregate and per customer.

15	What is an appropriate enforcement mechanism for a ransomware reporting obligation?	Ausgrid recommends that any entities not complying with obligations should be investigated by the Government and where appropriate have penalties imposed under the SOCI Act.
16	What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?	Tools, Techniques, Procedures (**TTP**) are the key information organisations will need to help prevent future incidents. We recommend that the Government issue a regular circular with updates to entities to ensure they can stay abreast of incidents.
Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator		
17	What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?	Ausgrid recommends that the information be sufficient to identify the threat actor and detail their activities, and the steps taken by the entity in response to and recovery from the incident.
18	What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?	Ausgrid recommends that all parties should deidentify information and none of it should be able to be attributable to customers or entities.
19	What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?	Government will need to position itself as a trusted actor to receive the information and share it in an anonymised and deidentified manner to encourage future sharing.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board		
20	What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?	Ausgrid recommends that the CIRB's purpose and scope should be to provide a realistic view of the cyber security challenges faced by Australian businesses. It should also review and assess significant cyber incidents and provide recommendations to Government based on members' breadth of expertise to drive improvement Australia's cyber resilience. The Government could model this off the US Cyber Safety Review Board Charter (cisa.gov).
21	What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?	Ausgrid recommends that any powers the CIRB has to collect information should be on a non-compliance and non-punitive basis. The CIRB should also not be able to store information for indefinite periods and should only be able to collect deidentified information.
22	How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?	See Ausgrid's response to question 14 above.
23	What factors would make a cyber incident worth reviewing by a CIRB?	Ausgrid recommends that the CIRB should review incidents that have caused a sustained disruption to business-critical functions of greater than 4 hours, aligned with the Australian Energy Sector Cyber Security Framework (**AESCSF**) definition for a critical infrastructure operator that can be attributed to a cyber-related trigger.
24	Who should be a member of a CIRB? How should these members be appointed?	Ausgrid recommends that CIRB members include industry representation from the energy sector. For example a nominee from the Trusted Information Sharing Network (**TISN**) energy sector group. We recommend members have a term of 3 years and can be reappointed no more than 2 times.
25	What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?	Ausgrid recommends representation with energy network experience. This should include Industrial Control Automation System (**ICAS**) or equivalent experience and qualifications.
26	How should the Government manage issues of personnel security and conflicts of interest?	Ausgrid recommends that CIRB member be vetted for negative vetting level 1 by the Government. In addition, standard personnel security and conflict of interest occur ahead of meetings. For example, declare and minute.
27	Who should chair a CIRB?	Ausgrid recommends a rotating Chair position with secretarial support from the Government.

28	Who should be responsible for initiating reviews to be undertaken by a CIRB?	Ausgrid suggests that the CIRB or Government could initiate a CIRB review. The CIRB's terms of reference would ensure that it is based on a reasonableness threshold or if the CIRB or Government identifies a new vector of attack. The CIRB should also provide business with TPPs for a new vector as part of its review.
29	What powers should a CIRB be given to effectively perform its functions?	Ausgrid recommends that the CIRB should have power to seek information but not have the power to compel information from entities. This should mirror other consultative government bodies like the Australian Cyber Security Centre.
30	To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?	Ausgrid recommends that the CIRB is covered by a limited use obligation so that report sharing is limited to relevant sector players.
31	What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?	Ausgrid recommends that the CIRB's information gathering powers be less stringent initially and increase over time as entities become more accustomed to its functions. However, as noted in our response to question 29, this should be limited to information seeking and not information compelling powers.
32	What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?	Ausgrid recommends that the CIRB include members from different industries and ensure its membership is diverse.
33	What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?	Ausgrid recommends that the Government implement secure systems for information transfer suitable for 'protected' level or above.
Measure 5: Protecting critical infrastructure – Data storage systems and business critical data		
34	How are you currently managing risks to your corporate networks and systems holding business critical data?	Ausgrid intends to manage its risks consistent with AESCSF version 2.0, security profile 3. However, this is contingent on the amount of cyber security funding approved by the Australian Energy Regulator (**AER**) for our 2024-29 regulatory control period. The AER is expected to publish its determination in April 2024. Ausgrid's November 2023 Revised Proposal included a program of controls to enable Ausgrid to achieve security profile 3. Ausgrid has also established a Certified Risk Management Professional role and is taking an ISO31000 risk based view of controls. This is aligned with Control Objectives for Information and Related Technology (**COBIT**) to mitigate risks to a defined appetite statement.

35	How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?	Ausgrid recommends that the Government amend the SOCI Act to require certification levels for Australian cloud data centres. This would help to align obligations between business customer intelligence and business data capabilities.
36	What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?	Ausgrid estimates that there will be financial and non-financial impacts of the proposed SOCI Act amendments. For example, depending on the obligations it is likely to result in additional reporting, systems and process.
Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers		
37	How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?	Ausgrid considers that providing the Government with powers to enable a temporary media embargo about the threat actor involved in the incident. This could assist in preliminary coordination and response to cyber incidents, including government actions against the threat actor.
38	What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?	Ausgrid must comply with strict Critical Infrastructure Licence Conditions under our New South Wales Distributor's Licence, which is issued under the *Electricity Supply Act, 1995 (NSW).* We understand that NSW's Independent Pricing and Regulatory Tribunal is seeking to align these obligations.
39	What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?	See Ausgrid's response to recommendation 37.
Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions		
40	How can the current information sharing regime under the SOCI Act be improved?	See Ausgrid's response to question 16. Ausgrid notes that calls to action to date have lacked sufficient clarity to provide entities with enough knowledge on how to act in response.
41	How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?	Ausgrid strongly supports the Government moving towards a "harm-based" approach.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers		
42	How would the proposed review and remedy power impact your approach to preventative risk?	Ausgrid is already committed to implementing risk management obligations within our organisation so far as reasonably possible and in line with the SOCI Act and does not anticipate enforcement impacting our approach to preventative risk management.
Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act		
43	What security standards are most relevant for the development of an RMP?	Nil comment.
44	How do other state, territory or Commonwealth requirements interact with the development of an RMP?	Nil comment.
45	How can outlining material risks help you adopt a more uniform approach to the notification obligation?	Nil comment.
46	What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?	Nil comment.
47	How do your procurement and network change management processes align with the existing and proposed notification arrangements? Can you suggest improvements to accommodate industry practice?	Nil comment.