29 February 2024

Hamish Hansford
Deputy Secretary
Cyber and Infrastructure Security Group
Department of Home Affairs

Submitted online: www.homeaffairs.gov.au

Dear Mr Hansford,

CYBER SECURITY LEGISLATIVE REFORMS

Origin Energy Limited (Origin) welcomes the opportunity to provide feedback on the Department of Home Affairs' consultation on the proposed new cyber security legislation and changes to the Security of Critical Infrastructure (SOCI) Act 2018. Our comments focus on areas where better safeguards, mechanisms or clarity could be provided to ensure the changes, if implemented, improve cyber security outcomes. Our main points are summarised below and more detailed responses to the consultation paper are provided in Attachment I.

New cyber security legislation

- Mandatory standards for smart consumer devices: An incremental implementation approach, such as legislating the first three principles of the proposed new standard, would be prudent given that mandatory standards for smart devices across the globe are a relatively new development. Responsibility for meeting the standards should fall to the entity that is best placed to manage this, including manufacturers, importers, or suppliers, as appropriate.
- Ransomware incident and payment reporting obligations: More information on the 'no-fault' and 'no-liability' principles would be useful to ensure stakeholders understand how they would be applied. This would provide confidence on their effectiveness in shielding entities from prosecution or compliance action when providing ransomware reports.
- Limited use obligation on information shared voluntarily: To achieve its intent of promoting voluntary information sharing, the scope of the limited use obligation should be narrowed, including by further restricting how the information can be used and with whom it can be subsequently shared.
- A Cyber Incident Review Board (CIRB): If the CIRB is introduced, it will be critical that its findings are not used to determine fault or liability. More information on how the proposed 'no-fault' principle would work would be useful to give entities assurance that it could be robustly and unambiguously applied.

Amendments to the SOCI Act

- Capturing business critical data that affect critical infrastructure: The legislation should be clear that this change would only affect systems that hold business critical data where these have a relevant impact on existing critical infrastructure assets. This would provide confidence that it is not intended to apply to all systems across an entity's business as this would create undue regulatory burden.
- Direction powers to manage consequences of cyber security incidents: If the Department proceeds with this power, strong safeguards and oversight mechanisms should be in place to ensure that the measure is only triggered as a last resort and that there are clear boundaries around what constitutes a "consequence" of an incident.
- A harms-based approach to help clarify when protected information can be disclosed: More guidance around what "harms-based" means could be included in the sector-specific rules to provide additional clarity. Alternatively, a more prescriptive frameworks approach could be

considered whereby the rules would set out a clear process that entities would then follow to decide if they can disclose information.

- Formal review and remedy powers to address seriously deficient risk management programs: We seek more information on how the review power would work, including how the relevant agency would determine that a program is seriously deficient. This may be difficult to achieve in practice given that the exact content of these programs is not prescribed to reflect that entities are best placed to manage their organisations' cyber security risks.

Should you have any questions or wish to discuss this submission further, please contact me at [redacted].

Yours sincerely,

Sarah-Jane Derby
Senior Manager, Regulatory Policy

Part 1 – New cyber security legislation

Measure 1: Secure-by-design standards for Internet of Things (IoT) devices

This measure proposes to adopt international security standards for consumer-grade IoT devices in order to be step with the international market.

Standards to be adopted in Australia

The proposal to use the existing UK approach (namely, ETSI EN 303 645) as a baseline for Australia is appropriate. Standards for smart consumer devices are a relatively nascent area and we understand that they have yet to be fully implemented across the globe. As a result, legislating the first three principles of ETSI EN 303 645 might be a prudent and incremental approach to implementation, particularly given the breadth of consumer products that would be captured under this proposal. Once standards become more common globally and more information is available on how the international market has adjusted to meeting these standards, consideration could then be given to extending the obligation. This could include additional principles or standards (such as ISO/IEC 27001) to ensure access to a secure supply chain of consumer-grade products.

Responsible entities

As a rule, responsibility for meeting the standards should fall to the entity that is best placed to manage this, including manufacturers, importers, or suppliers, as appropriate. We broadly agree with the option to use the approach taken for consumer product safety as a baseline for determining responsible entities. Consumer product safety requires vendors, suppliers, importers and manufacturers to comply with the standard before products can be supplied into the Australian market. This appears consistent with our comments above about who should bear responsibility.

Smart devices to be regulated

We understand that consumer-grade devices relevant to the energy sector would largely be exempt due to other work being undertaken to introduce standards for solar inverters, home battery systems and electric vehicles (EVs).[1]

With the growth of consumer energy resources (CER) in the electricity sector, other consumer-grade devices relevant to the energy industry (such as devices that may be used in Virtual Power Plants) could be captured by this new proposal. Clarity would be welcome on whether devices relevant to the energy sector other than solar inverters, home battery systems and EVs would be captured through the new cyber security laws or other work being done by the Government. In any case, our preference is for consistent standards to apply across these consumer-grade devices to minimise regulatory burden.

Measure 2: Ransomware reporting for businesses

This measure would establish a new 'no-fault' and 'no-liability' ransomware reporting obligation on an entity if:

1. it is impacted by a ransomware or cyber extortion attack and receives a demand to make a payment.
2. if an entity makes a payment.

[1] See https://cybersecuritycrc.org.au/sites/default/files/2023-11/3320_cscrc_powerout_art_web.pdf

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo, Sydney NSW 2000
GPO Box 5376 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

Which entities are required to report

Regulated entities under the existing SOCI Act may be subject to mandatory cyber incident reporting requirements, including ransomware or cyber extortion attacks. We understand that entities that are subject to this requirement could be exempt from the first limb of the new proposed reporting obligation. This would be appropriate to minimise regulatory burden since the new obligation would duplicate the existing requirement.

Sharing ransomware reporting information

This measure includes a proposal to share information (including anonymised sensitive information) on ransomware incidents through a publicly released quarterly report, as well as industry or sector-specific reports.

In considering this, the Department should have regard to whether sensitive, commercial or confidential information can be genuinely anonymised through this process; and whether there could be unintended consequences from publishing ransomware information. For example, major cyber security incidents including where ransomware payments are made are likely to be rare but very public. It is not clear if the sample size for these types of events would be large enough to allow for information to be anonymised or published in such a way that the public would not be able to infer sensitive details from the reports or use the information to assign fault.

'No-fault' and 'no liability' protection principles

The consultation paper states that 'no-fault' aims to provide assurance to entities that the agency receiving ransomware reports under this obligation will not seek to apportion blame for the incident. It would be useful to understand how this would be applied, particularly given that this measure also includes a proposal to share information around ransomware reporting publicly, which means the data could be made available to other regulatory bodies.

With respect to the 'no-liability' principle, the consultation paper notes that its intent would be to provide confidence for entities that they will not be prosecuted for making a payment. More information on the scope of this principle would be useful to understand its reach and limitations, such as which legislation or regulatory frameworks would be captured by this principle. As an example, there could be a situation whereby a payment is made to a cybercriminal from a country subject to the sanctions regime.[2] It is unclear if the entity making the payment could be subject to penalties or prosecution under that regime, or whether entities would be shielded from this due to the 'no-liability' principle.

Timeframes for reporting

To minimise regulatory burden, we suggest that timeframes for reporting a ransomware or cyber extortion attack should align with existing SOCI obligations for mandatory cyber incident reporting.

Measure 3: Limited use obligations on the Australian Signals Directorate (ASD) and the National Cyber Security Coordinator (NCSC)

This measure would introduce limited use obligations. This would mean that information shared with ASD or the NCSC could only be used for specific purposes defined in the legislation ("prescribed cyber security purposes") so that regulatory agencies could not use this information for compliance action.

[2] Australian sanction laws implement United Nations Security Council (UNSC) sanctions regimes and Australian autonomous sanctions regimes. See https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo, Sydney NSW 2000
GPO Box 5376 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

Origin considers that the obligation and specifically, the limits proposed in the consultation paper (i.e. the "prescribed cyber security purposes") are too broad and may not achieve the Department's intended aim of further promoting voluntary information sharing with the ASD and NCSC.

To promote sharing, the obligation should be strictly restricted to provide confidence that the information is not used for purposes it is not intended for, such as for compliance action. For example:

- The obligation could be improved by further restricting what is included in the definition of "prescribed cyber security purposes". Limited use could focus on managing an incident only.
- The Department should consider further restricting who the information could be shared with compared to what is proposed in the consultation paper.
- If information is shared with other agencies and departments, the obligation should require the ASD to first seek consent from entities to do so before any information can be shared.

Measure 4: A Cyber Incident Review Board

This measure proposes to establish a Cyber Incident Review Board (CIRB). The CIRB would conduct no-fault incident reviews to reflect on lessons learnt from cyber incidents and share these with the public.

'No-fault' principle

The consultation paper references the independent 'no blame' review process that the Australian Transport Safety Bureau (ATSB) has in place to investigate transport-related incidents and accidents, as a potential model for the CIRB. If the CIRB is introduced, the 'no blame' / 'no-fault' approach will be critical to ensure that the outcomes of the reviews would not directly or indirectly provide the means to determine fault or liability for a cyber security event. More information is therefore needed on how the approach would work in practice to give entities assurance that the 'no-fault' principle could be robustly and unambiguously applied.

Functions of the CIRB / Protecting sensitive information

While we understand that sharing lessons learnt could be of value to industry, the challenge remains that detailed information about an entity, including potentially sensitive information that would not have otherwise been available to the media or the public, would be shared publicly through the incident reports.

One way to manage this might be to focus on a series of incidents rather than one; however, as previously noted, major cyber security incidents tend to be rare and very public. Given this, it is not clear that this can practically be achieved without entity-specific sensitive information being inferred from the reports. Redacting sensitive information might also be an option but would need to be balanced against the usefulness of publicly releasing redacted reports. These issues should be considered by the Department before establishing a CIRB.

CIRB governance

Governance of the CIRB will be crucial to ensure that it can impartially conduct reviews without the aim of assigning blame. The Chair should therefore be fully independent from Government and any regulatory agency.

Investigatory powers

The consultation paper states that the CIRB could have voluntary powers to request information but no powers to compel entities to participate in reviews; or alternatively, the CIRB could have limited

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo, Sydney NSW 2000
GPO Box 5376 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

information gathering powers to require entities to provide appropriate information. The paper also notes that the CIRB, if given information gathering powers, may need to be covered by a limited use obligation. As noted under measure 3, limited use obligations need to be narrow in scope to give entities confidence of their effectiveness. For the CIRB, voluntary powers would be preferable to limited information gathering powers, particularly given our concerns above around protecting sensitive information.

Part 2 – Amendments to the SOCI Act

Measure 5: Data storage systems and business critical data

This measure aims to change the definition of "asset" in the SOCI Act and "material risks" in the critical infrastructure risk management program (CIRMP) rules to capture "data storage systems that hold business critical data".

Scope of application

We understand the intent of this change is to address a minor gap in the existing legislation to capture systems that hold business critical data and that support critical infrastructure assets and is not intended to introduce wholesale changes to the classes of critical infrastructure assets captured by the SOCI Act.

Large businesses often operate distinct units or subsidiaries, and only some parts of their organisation may operate assets that are classified as critical infrastructure. Other parts of the organisation may use systems that hold data that is critical to their business units, but these systems would not have a relevant impact on critical infrastructure assets. Our understanding is that this proposed change is only intended to expand the systems that directly affect existing critical infrastructure assets, rather than capture additional systems in other parts of the business.

Including these additional systems would represent a significant change to the SOCI Act rather than plugging a minor gap. It would create undue regulatory burden on entities with no additional benefit to managing risks to critical infrastructure assets. Clarity on this aspect would be useful in the legislation and CIRMP rules.

Relationship with the Privacy Act

If the Department is concerned about safeguarding personal information data beyond systems that affect critical infrastructure assets, then it would be more appropriate to consider changes to the Privacy Act if deficiencies are found. This would also help to minimise duplication since the Privacy Act already covers requirements for protecting personal information.

Measure 6: Consequence management powers

This measure proposes to introduce an all-hazards, last resort consequence management power integrated within existing government assistance powers.

We consider that this measure is broad in scope and would in effect introduce direction powers for entities that may not be directly involved in an incident. Therefore, if the Department proceeds with this consequence management power, safeguards and oversight mechanisms should be in place to ensure that the measure is only used as a last resort and that there are clear boundaries around its use such that the scope of application is narrow.

Last resort power

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo, Sydney NSW 2000
GPO Box 5376 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

We understand that the existing Government assistance measures have not been used to date, consistent with the intent of these types of measures being last resort powers. The legislation should be clear that the consequence management measure would also be a last resort power. Prior to exercising this power, the legislation should first require extensive engagement and consultation with all relevant participants to manage an incident and its consequences through a collaborative process.

Clear boundaries

We understand that existing Government assistance measures are limited to "cyber security incidents" which provides a clear boundary around when it can be used. This proposal would extend Ministerial direction powers to addressing a "consequence of an event" which has a relevant impact on critical infrastructure. This could be broad in application.

We consider that a narrower trigger for the use of this power would be preferable, specifically around the definition of "consequence of an event". The consultation paper does note that "to be considered for use, the consequence/s this power seeks to address must have a causal link to an incident impacting a critical infrastructure asset". However, this remains subject to interpretation and does not set clear boundaries on its use. More guidance around what is meant by causal link and which types of consequences could be captured by this power would be useful to give entities confidence around its limited use.

Interactions with other direction powers

The Department should consider the risk of conflict across different Government intervention frameworks. For example, energy sector entities might be subject to direction powers by other entities such as AEMO, ACCC or the AER, noting this could also occur under the existing SOCI Government assistance measures. For example, this could lead to a situation where the Government directs a plant to temporarily cease production to manage the consequence of a cyber incident while AEMO directs a plant to ramp up output to avoid blackouts. It is critical therefore that the legislation includes steps for coordination across all the relevant entities to minimise the potential for conflicting instructions.

Measure 7: Protected information provisions

This measure proposes to clarify that entities should take a harms-based approach when disclosing information under the SOCI Act to promote information sharing.

We agree that there is a need to improve the current information sharing regime under the SOCI Act. Lack of clarity around disclosure of protected information can hinder efficient management of risks, e.g., due to uncertainty around whether relevant information can be shared.

A harms-based approach

While a harms-based approach might represent an incremental improvement on the existing arrangements, we consider that more prescription would be necessary to ensure it does provide more clarity for stakeholders so that entities can more easily determine if information held can be disclosed. For example:

- More guidance around what "harms-based" means could be set out in the sector-specific rules to provide additional clarity.
- Alternatively, a more prescriptive frameworks approach could be considered whereby the rules (or legislation) could set out a clear process that entities would follow to decide if they can disclose information.

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo, Sydney NSW 2000
GPO Box 5376 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

In addition to the above, consideration should be given to explicitly excluding information that can be deduced from publicly available data from being classified as protected information under the Act. This would promote sharing of information that would, indirectly, already be in the public domain.

Clarification of disclosure provisions

The measure also includes a proposal to broaden the disclosure of protected information to all Commonwealth, state and territory government entities regardless of policy responsibility, where disclosure is necessary for the purpose of upholding the security and resilience of critical infrastructure or protecting national security. Currently, the Secretary of Home Affairs may disclose protected information to a limited range of ministers and agencies.

Sharing information across a broader range of agencies and departments may lead to unintended consequences, such as multiple distinct entities taking the lead on managing a particular incident in isolation of one another, once they have access to protected information. This could make managing cyber security incidents less efficient. As a result, we consider the legislation should have safeguards in place to ensure that:

- Consent from entities is requested prior to sharing their protected information with other agencies.
- There are clear lines of responsibilities and strong coordination with respect to event management to ensure incidents can be managed efficiently.

Measure 8: Review and remedy powers

This measure proposes to introduce a formal, written directions power to address seriously deficient elements of CIRMPs.

We understand that the Department is concerned that the lack of a regulatory regime to require an entity to address deficiencies in the CIRMP means the program may not achieve its intent. However, it is not clear how significant the lack of a formal review and remedy power is given that the SOCI Act includes an oversight process (via a Board attestation requirement) which was introduced to ensure that CIRMPs are fit for purpose and of good standard. More information on whether the Department considers this process is not adequate or sufficient would be useful.

Review power

The consultation paper does not provide any information on how the review power would work, only that the Secretary of Home Affairs or relevant Commonwealth regulator would "consider the facts and the entity's obligations under the SOCI Act and delegated legislation" to form "a reasonable belief that an entities' CIRMP is seriously deficient". We would welcome more information on the review power and how it is intended to work, in particular, how the relevant agency would determine that a CIRMP is seriously deficient.

A review power for CIRMPs could be difficult to implement in practice. CIRMPs are, under the existing legislation, intended to be bespoke and flexible programs to allow each entity to determine how to manage its organisation's cyber security risks, as it is best placed to do so. As a result, it would be difficult for an individual CIRMP to be objectively reviewed by a regulatory or independent body without a clear benchmark or mandated parameters. In a practical sense, an objective review could only be achieved if the content of CIRMPs become more prescriptive, which would be inconsistent with how entities manage cyber security risks. A more prescriptive CIRMP would be a significant change to the SOCI Act, and disproportionate to the problem statement. It might create additional regulatory burden if

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo, Sydney NSW 2000
GPO Box 5376 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

existing CIRMPs need to be significantly amended. These issues should be considered by the Department in implementing this power.

Safeguards

If the review and remedy powers are introduced, clear guidance will be necessary as well as strong safeguards to ensure these powers are used as a last resort only. For example:

- The legislation should require the agency responsible for reviewing CIRMPs to first work collaboratively with the entity to provide feedback on and change CIRMPs. Entities should then be given ample time to address their CIRMPs before the remedy powers are used.
- The powers could be limited to instances where there is an imminent threat to security, or include other restrictions on its use to ensure it is a last resort option.

We also agree with the oversight mechanisms proposed in the consultation paper, such as written notice of intent to issue a direction to remedy a deficiency and consultation on this notice.

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo, Sydney NSW 2000
GPO Box 5376 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au