16 September 2020

Department of Home Affairs
email: ci.reforms@homeaffairs.gov.au

Protecting critical infrastructure and systems of national significance

CitiPower, Powercor, United Energy and SA Power Networks welcome the opportunity to make a submission on the consultation paper *Protecting critical infrastructure and systems of national significance* which proposes a new framework for uplifting the security and resilience of Australia's critical infrastructure.

In summary, we support:

- embedding a risk-based approach to managing security risk for critical infrastructure
- defining the scope of the regulatory regime to only capture the assets and systems for which unauthorised access poses a national security risk. That is, the assets and systems that monitor and control electrified assets (i.e. our operational technology)
- leveraging existing industry security frameworks to minimise duplication and undue cost, as well as ensuring consistency in frameworks across jurisdictions and consistency of definitions across legislative instruments
- ensuring the compliance and enforcement regime reflects the risk-based framework
- consideration of the government providing a centralised threat intelligence service through the collection of threats or incidents relating to critical infrastructure and ensuring dissemination of the information back to critical infrastructure providers
- very carefully prescribing and limiting the circumstances in which government may impose directions on critical infrastructure. The Government should not be able to take direct control of an electricity network under any circumstance due to the very high safety risks.

As a critical infrastructure provider, we appreciate the opportunity to engage in the development of a nationally consistent framework for managing security risk. We understand this initial consultation discusses the new framework at a concept level, with many details to be worked through in due course. We anticipate more opportunities for us to engage in the development of the detailed regulatory requirements and the compliance and enforcement framework.

Please feel free to contact the following if you have any queries regarding our submission:

- Megan Willcox, Manager Regulatory Projects, on [redacted] or [redacted]
- Luke Gidiuli, Manager , on [redacted] or [redacted]
- Nathan Morelli, Manager Cyber Security, on [redacted] or [redacted]

Best regards

[redacted]

Renate Vogt
General Manager Regulation
CitiPower, Powercor Australia, United Energy

[redacted]

Chris Ford
General Manager Innovation & Technology
SA Power Networks

1.1 Embed a risk-based approach and clearly define the scope of assets subject to regulation

We strongly support applying a risk-based framework for regulating the security capabilities of critical infrastructure providers. A risk-based approach appropriately balances the need to mitigate security risks with the cost to the Australian public. A risk-based regulatory approach is also consistent with our general obligations in relation to maintaining safety and reliability of the electricity network.

The key to a successful risk-based framework is not to prescribe 'how' risk is addressed, instead requiring demonstrating that we have identified and managed risk to an acceptable level. Importantly, if specific security outcomes are the policy goal, then the regulation should be focussed on the outcome sought, in terms of appropriate residual risk levels, and not the input, solution or approach for achieving that outcome.

We already adopt a risk-based approach for determining the appropriate physical and cyber security measures across our business operations. Notably, we apply stronger security measures for the protection of electrified assets and IT/OT systems which monitor and control electrified assets. These systems pose greater risk of security threats and have more significant consequences of unauthorised access, compared with non-electrified assets and our corporate IT systems.

To ensure the proposed regulatory framework does not overreach its intended purpose of protecting national security, we recommend the scope of regulation be defined to only capture the assets and systems for which unauthorised access poses a national security risk. That is, the assets and systems that monitor and control electrified assets (i.e. our operational technology).

We would not expect our corporate systems to be subject to the proposed new regulatory reporting arrangements, as these systems are similar to those deployed in any non-critical infrastructure business and do not pose the same level of risk or consequence of unauthorised access. We recognise however the need to ensure we have adequate security measures to ring-fence access between our IT and OT systems.

Including all assets and systems of a critical infrastructure entity in the new regulatory framework would unduly increase the regulatory burden, and increase costs to customers, beyond that necessary to mitigate national security threats. A targeted risk-based regulatory framework therefore ensures the level of regulation of security measures is commensurate with the extent of risk and consequence and costs to customers is warranted.

1.2 Leverage existing industry frameworks

We support leveraging existing industry security frameworks as the basis for critical infrastructure providers to demonstrate compliance with the proposed positive security obligations. Leverage existing industry security frameworks will minimise the costs of implementing the new proposed regulatory framework for protecting critical infrastructure. Many critical infrastructure providers have already adopted the industry frameworks and embedded these into the operations and internal reporting processes.

Examples relevant to electricity distribution networks include:

- the Australian Energy Market Operator's **Australian Energy Sector Cyber Security Framework** (AESCSF). The core framework is mapped to National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), and cross references the relevant global and Australian Cybersecurity best practices and standards e.g. Australian Cyber Security Centre (ACSC) Essential 8 and ISM, Australian Privacy Principles, ISO27001, etc. The framework has a Criticality Assessment Tool (CAT) that provides necessary guidance to assess each market participant against a set of predefined criteria to determine their relative criticality to the sector
- Energy Networks Association's **National guidelines for prevention of unauthorised access to electricity infrastructure** – provides a risk-based framework for the protection of physical assets for electricity networks.

1.3 Ensure consistent definitions across legislative instruments

We consider the definition of critical infrastructure, set out in section 10 of the Security of Critical Infrastructure Act 2018, as it relates to electricity distribution, is still fit for purpose.

We note there is misaligned of definitions across national and state legislation which may present interpretation conflicts when operationalising the proposed new framework for protecting critical infrastructure and systems of national significance. The following examples are relevant:

- the Security of Critical Infrastructure Act 2018, includes definitions of *'critical infrastructure asset'*, '*critical electricity asset*' and '*responsible entity*'
- the Victoria Emergency Management Amendment (Critical Infrastructure Resilience) Act 2014 includes definitions of '*critical infrastructure*' '*major critical infrastructure*' '*significant critical infrastructure'* and '*essential service*'
- the South Emergency Management Act 2004 (Version: 24.7.2020), and The State Emergency Management Plan (SEMP) as prepared under section 9(1)(b) of the Act, includes a definition of '*critical infrastructure'.*

Further, existing industry frameworks currently adopted for managing the security of critical infrastructure may have further variations in definitions.

The implementation of this new framework presents an opportunity to harmonise, as far as possible, definitions of critical infrastructure. This could potentially be tabled with and considered by newly established National Federation Reform Council and relevant sub-committees for energy and/or infrastructure and transport.

1.4 Ensure compliance and enforcement regime reflects a risk-based approach

Upholding the principle of a risk-based framework is heavily reliant on the manner in which compliance with the framework is assessed by the Regulator. An overly prescriptive approach to demonstrating and reporting on compliance can inadvertently result in a more deterministic implementation of the framework. As noted above, this would undermine the benefits of a risk-based framework, most notably that the costs to customers only reflect those necessary to effectively mitigate security risks. Further, it may also lead to a one-size fits all approach, potentially inhibiting innovations in security initiatives, and resulting in wide scale vulnerabilities.

Further, an overly cumbersome and prescriptive reporting and assessment regime would result in higher costs to both the critical infrastructure providers and the Regulator. These costs would ultimately be borne by electricity consumers and the broader Australian public.

We recommend the following measures would assist in upholding the principle of risk-based regime:

- ensuring the Regulator is well equipped and experienced in administering a risk-based framework
- ensuring the regulatory framework prescribes the compliance assessment approach must be sufficiently flexible to enable different entities to use different approaches to demonstrate their initiatives meet the objectives of mitigating security risks to the level proportionate to the relevant risks and consequences
- in setting any reporting obligations and undertaking compliance assessments, the Regulator must have regard to:
  - the different means by which entities may demonstrate compliance with the framework
  - the outcomes achieved, in terms of risks and consequence mitigation, rather than the solution adopted.
- in determining the enforcement response, the Regulator must have regard to the level of residual security risk and consequence not adequately addressed by the entity, as well as the extent of repetition and intention in the entities behaviour.

We suggest the Critical Infrastructure Centre (**CIC**) may be an appropriate body for enforcing the proposed risk-based regulatory regime. The CIC would provide a single lens across the many different industries classified as critical infrastructure, ensuring the level of regulatory prescription for any particular industry aligned with its level of criticality to national significance.

1.5 Development of a centralised threat intelligence service

There is an opportunity for the government to support critical infrastructure entities security efforts by providing a centralised threat intelligence service. For example the Government could coordinate the collection and dissemination of unauthorised access threats or incidents involving physical or IT/OT systems of critical infrastructure.

A new centralised threat intelligence service should consolidate the existing services such as the Australian Cyber Security Centre and the Joint Cyber Security Centre, to avoid duplication of reporting and resources. Importantly, there should be a two-way flow of information between government and critical infrastructure providers.

A centralised, government coordinated, threat intelligence service would ensure all market participants are able to respond in a timely fashion to new threat intelligence information. Currently each participant pays for their own information services, which makes it an uneven playing field and may disadvantage some participants from accessing the information they need to effectively manage risks. We consider a centralised approach would be consistent with the National cybersecurity strategy position – where Government is responsible for managing threats and we are responsible for protecting our assets.

1.6 Carefully prescribe and limit government control

Government rights to direct actions of critical infrastructure assets should be tightly defined and limited to:

- emergency situations of threat to national sovereignty; and
- last resort measures – where all other means have been exhausted or considered ineffective to address the threat.

Government should not, under any circumstance, take direct control of critical infrastructure assets, especially electricity networks as the risk to public safety is too high.

As operators of electrified assets located throughout public and private locations, we must ensure, above all else, the safety of our electrical assets, our personnel and the public. We have highly trained specialist skilled field and control room personnel whose first priority is to ensure electrical safety, including our life support customers are protected and our field crew know which assets are energised. Therefore, any Government direction of the electricity network must only be of the utmost importance to national security, and Government direct control of assets should not be permitted under any circumstance.

We note the consultation paper refers to 'robust checks and balances being put in place' we agree these are needed and would welcome additional clarity regarding what these would likely involve. Further, we would expect the Government to resume responsibility for any unintended consequences of such emergency directions, including compensating persons who suffer loss as a result.

Importantly, we are constantly working directly with emergency services, including the fire services, ambulance services and police to ensure their objectives are met in emergency situations, while upholding the integrity and safety of our electrical assets. We will not hesitate to work closely with Government to protect national security, while maintaining the safety of the electrical network for our employees, customers and public.

1.7 Enhanced security provisions for systems of national significance

It is difficult to comment on the appropriateness and cost implications of the proposed enhanced security provisions without more detail in relation to:

- situation awareness - the type, frequency and extent of information that would be required to be shared and through what avenues?
- preparatory activities - the level of resource required to engage in the proposed preparatory activities and development of a national playbook. It is also unclear whether these activities would lead to mandated requirements on critical infrastructure entities security measures, for example would the national playbook be mandated and supersede our own playbooks? Would the outcomes of third party reviews result in mandated changes to our security operations? We have some concern that a mandated playbook deployed across an industry could inadvertently introduce security vulnerabilities.