NSW Government Submission

Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

10 September 2020

Table of Contents Page

Executive summary

1. Protecting Australia's critical infrastructure is a shared responsibility and the NSW Government is committed to working with the Commonwealth to protect the essential services all Australians rely on.
2. NSW is supportive of the intent of the proposed framework. However, NSW reiterates our concerns over the short timeframe for submissions, particularly given the significance of the proposed legislation and the co-operative approach that is required for the legislation to be effective in practice.
3. The NSW Critical Infrastructure Resilience Strategy 2018 supports the protection of critical infrastructure in NSW. This Strategy was developed in partnership with the NSW community and infrastructure owners and operators. It is designed to improve infrastructure resilience, organisational resilience and community resilience.
4. Work is continuing in NSW to enhance our state-based critical infrastructure framework. Infrastructure NSW has recently partnered with Infrastructure Australia to identify actions needed to improve critical infrastructure resilience. Preliminary findings indicate that regulation is likely needed to ensure that governments better understand the state of readiness to human or natural hazards of critical infrastructure providers, in particular privately owned and operated infrastructure, including telecommunication and energy infrastructure.
5. This aligns with the recent findings of the NSW Bushfire Inquiry, which recommended that Australian governments revise the regulatory framework to provide information to Government on all critical infrastructure for appropriate planning and response to bushfires. The NSW Government has accepted all of the Inquiry's recommendations.
6. Cyber Security NSW continues to undertake critical work to reduce NSW's exposure to cyber threats. It has worked over the past year on capability building and response coordination across the NSW public sector. A key focus has been the implementation of the mandatory requirements as outlined in the NSW Cyber Security Policy (CSP).
7. The NSW Government has also begun work to review and update processes for the identification and classification of critical infrastructure in NSW across the counter terrorism and emergency management contexts. Existing regulatory regimes, including any changes implemented in NSW as a result of the existing NSW review project, should not be duplicated.
8. As identified in the Consultation Paper, a range of hazards have the potential to significantly compromise the supply of essential services across Australia. In the wake of the 2019-20 bushfires and the COVID-19 pandemic, NSW recognises the need to protect Australia's critical infrastructure from all hazards.
9. It is noted the Consultation Paper builds on work undertaken for the development of Australia's Cyber Security Strategy. In line with the proposed all hazards approach, an increase in focus on cyber security should not result in a re-direction of resources away from existing counter terrorism and emergency management efforts to protect critical infrastructure.
10. Noting the proposed framework's coverage across sectors, and proposed thresholds for regulation, the regulatory impact of these reforms may be significant. It remains unclear if any Commonwealth resourcing will be made available to support the implementation of the proposed framework, including increased auditing to ensure compliance.
11. The NSW Government asks the Department of Home Affairs to clarify what reforms are being developed in response to the following questions posed within the Consultation Paper:
    a. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

b. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

c. Who should oversee the Government's use of these powers?

12. The NSW Government notes that in certain limited circumstances, the Commonwealth is seeking to introduce a mechanism to intervene when an immediate and serious cyber threat to Australia's economy, security or sovereignty (including threat to life) is identified. NSW acknowledges the appropriateness of the power with respect to those critical infrastructure assets which may be privately owned and operated. However, NSW recommends that any emergency declaration or use of direct and coercive powers should only be done in a co-operative approach with the relevant State or Territory Minister.

13. It is noted that proposed enhancements to the critical infrastructure framework may result in greater information being reported directly to the Commonwealth. It is important that information-sharing arrangements with State and Territory Governments be clarified in the legislation to ensure jurisdictions are adequately informed of any issues in their jurisdiction.

14. This submission outlines preliminary responses to key targeted questions in the Consultation Paper. Significant further work is required to ensure alignment with existing policy and regulation in NSW and to ensure the proposed Commonwealth legislation is fit for purpose and proportionate across all sectors.

15. NSW looks forward to continued consultation and collaboration with the Commonwealth on the next stages of these important reforms.

Response to targeted questions in the Consultation Paper

Do you think the current definition of Critical Infrastructure is still fit for purpose?

The current definition of 'critical infrastructure' may unintentionally exclude some sectors and systems. In particular, the term 'information technologies' may limit the application of the SOCI Act by excluding operational technologies or those managed on third party platforms. The use of an industry recognised functional classification scheme for Information Technology / Operational Technology such as ISA-95 / IEC 62264 may assist in better targeting the obligations of the Act.

Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

The implementation of the new SOCI reforms should have regard to instances where public sector agencies are already achieving a higher level of cyber maturity under existing state government standards. Detailed mapping is required to understand where there may be additional financial costs and duplication associated with the imposition of new reporting obligations.

The NSW Government would appreciate the opportunity to participate in further consultation prior to these new reporting standards being finalised. In addition, extensive stakeholder consultation is required to ensure these existing obligations are not duplicated by any new Commonwealth obligations.

Over the last 12 months Cyber Security NSW has put significant resources into capability building and response coordination across the NSW public sector. A key focus has been the implementation of the mandatory requirements as outlined in the NSW Cyber Security Policy (CSP).

The principles-based outcomes outlined in the framework are consistent with the existing Mandatory Requirements in the NSW CSP. These requirements include the Australian Cyber Security Centre (ACSC) Essential 8.

The CSP does not prescribe mandatory maturity levels - these levels will be determined by the risk profile and risk appetite of each agency. Additional or duplicative principles could impose a significant time and/or financial cost on NSW agencies and entities, though more detail would be needed on the degree of overlap with existing reporting obligations.

In addition, the CSP requires NSW Government agencies and departments to identify and report on their 'crown jewels" (i.e. their most vital systems and services). The processes set up by NSW Government public sector agencies to identify and manage crown jewels systems and services can be incorporated with the SOCI reforms. The identification processes currently used includes a risk-based assessment of the critical assets and the other internal and external systems they connect to.

NSW public sector agencies are all uplifting their cyber security maturity as part of the implementation of the mandatory requirements in the NSW Cyber Security Policy. Additional or duplicative Commonwealth Government maturity targets could complicate or hinder existing NSW cyber security uplift efforts if they are not developed in a consultative way.

Based on an initial review of the draft definitions and thresholds, there will be a regulatory impact for NSW agencies if the proposed reforms are implemented, though the extent of this impact will be determined by the legislation and accompanying rules and regulations underpinning the legislation.

Regulatory impact will be reduced if State and Territory Governments are able to provide detailed input into the development of the legislation and supporting regulations.

In order to accurately map the regulatory impact these reforms would have on NSW entities, the Australian Government should release the draft legislation and regulations for close consultation with the NSW Government and NSW critical infrastructure owners and operators.

Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

A number of sectors in NSW are subject to security obligations in-line with the proposed principles. The NSW Cyber Security Policy requires government departments, statutory authorities and public service agencies to implement the mandatory requirements and ACSC Essential 8 controls.

Consultation with each agency and cluster is required to determine the associated costs with meeting existing cyber security reporting obligations.

Would the proposed regulatory model avoid duplication with existing oversight requirements?

The Government notes there is the potential for duplication if the legislation intends to include NSW government departments, Statutory Authorities and Public Service agencies. Based on the draft definitions and thresholds, NSW Telecommunications Authority critical communications, NSW Health/Local Health Districts and transport infrastructure will potentially have duplicated reporting obligations. Further discussions at the Commonwealth and State level is required to determine the extent of duplication with existing oversight requirements and any overlap that exists.

To avoid duplication of effort in reporting by owners and operators, the NSW Government should be able to access the consolidated holdings of information on critical infrastructure assets in NSW, including privately owned and operated assets.

Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

Jurisdictional central cyber security units, such as Cyber Security NSW, are best placed to undertake the regulatory role for state and territory government sectors included in the legislation's expansion. Any SOCI reform reporting requirements could be used by Cyber Security NSW as part of its broader cyber security maturity reporting processes.

This may require jurisdictions to expand the role and funding of central cyber security units. For example, the NSW Government is expanding the role of Cyber Security NSW and the expanded regulatory role is supported by the development of more compliance and audit functions as well as awareness, training and maturity uplift functions.

Cyber Security NSW will also be implementing NSW Government 'spot' audits in 2021, assessing the maturity ratings of clusters and agencies for a number of Mandatory Requirement and Essential 8

maturity assessments, and also undertaking Essential 8 uplift activities modelled on the uplift program of the ACSC.

Cyber Security NSW has explored options to include State-Owned Corporations (SOCs) under the scope of the CSP. To-date, SOCs are not required to implement the CSP, though are encouraged to.

However, for entities that fall outside of Cyber Security NSW's remit, the most appropriate regulator in a given sector should be based on extensive consultation with the impacted agencies and entities in each State and Department.

What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

The Consultation Paper indicates that infrastructure owners/operators will be required to report directly to the Commonwealth. This may result in State and Territory Governments being bypassed, and jurisdictions not being adequately informed of significant issues with critical infrastructure based in their jurisdiction. It is therefore important that information-sharing arrangements with State and Territory Governments be clarified in legislation.

Recent research undertaken by Infrastructure NSW with Infrastructure Australia indicates that the arrangements for sharing information needs improvement between infrastructure sectors and all levels of government. This work also identified that regulation is likely to be needed to ensure that governments better understand the state of readiness to human or natural hazards of critical infrastructure providers, in particular privately owned and operated infrastructure, including telecommunication and energy infrastructure.

This aligns with the recent findings of the NSW Bushfire Inquiry, which recommended that Australian governments revise the regulatory framework for information provision to government on all critical infrastructure for appropriate planning and response to bushfires (Recommendation 29). The NSW Government has accepted all of the Inquiry's recommendations.

What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

For any future playbooks to be effective, they must be developed in partnership between the Australian Government, state and territory governments, and industry sectors. The content of playbooks should be evidence-based, operationally-tested, and seek to set outcomes over prescriptive requirements.

Playbooks should be guided by existing materials created in this area. For example, the NSW Government is currently leading a taskforce to harmonise industry cyber security standards, in partnership with Standards Australia and the cyber security industry growth centre, AustCyber. The outputs of this taskforce will be the result of extensive national collaboration across key industry sectors and will provide a strong foundation on which to develop more detailed playbooks.

Playbooks must also consider existing State-level response arrangements. For example, these reforms may have unintended impacts on existing emergency management arrangements.

Comments on amendments to the *Security of Critical Infrastructure Act 2018*

The NSW Government provides the following comments on potential amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act).

Proposed legislative changes should:

- outline the roles and responsibilities of Commonwealth and State and Territory Governments;
- define what constitutes a function "vital to Australia's economy, security and sovereignty;"
- include a similar level of detail to the assets already captured by the SOCI Act for the 11 additional sectors;
- clearly articulate which industries are covered by the critical infrastructure reforms and note the relevant thresholds for when an entity becomes subject to legislation;
- include safeguards and oversight measures to ensure the necessary level of accountability for these type of powers (i.e. oversight similar to Inspector-General of Intelligence and Security, or Parliamentary Joint Committee on Intelligence and Security, or Reporting to Senate Standing Committee on Foreign Affairs, Defence and Trade);
- include indemnity against civil litigation (damages) when acting in good faith and within powers vested by the legislation;
- be drafted to consider upcoming and future technologies and innovations in critical infrastructure;
- clearly articulate the commitment to Commonwealth assistance; and
- address information-sharing arrangements with State and Territory Governments.

The legislation should not:

- duplicate State and Territory regulatory frameworks;
- constrain entities from managing risk using their own enterprise risk management frameworks and acceptance criteria; and
- constrain sector innovation.