Governance Institute of Australia

T +61 2 9223 5744 **F** +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

16 September 2020

Department of Home Affairs

By email: ci.reforms@homeaffairs.gov.au

Dear Sir/Madam

Protecting Critical Infrastructure and Systems of National Importance – Consultation Paper August 2020

Governance Institute of Australia (Governance Institute) is the only independent professional association with a sole focus on *whole-of-organisation* governance. Our education, support and networking opportunities for directors, company secretaries, governance professionals and risk managers are unrivalled.

Our members have primary responsibility for developing and implementing governance and risk frameworks in public listed, unlisted and private companies. Many of our members are working as governance and risk professionals in a range of organisations, from the largest listed companies responsible for critical infrastructure and systems of national importance to small businesses and not-for-profits. They are frequently those with the primary responsibility for dealing and communicating with regulators such as the Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA). In listed companies, they have primary responsibility for dealing with the Australian Securities Exchange (ASX) and interpreting and implementing the Listing Rules. Our members have a thorough working knowledge of the Corporations Act 2001 and also play an important role in external reporting by public listed, unlisted and private companies. We have drawn on their experience in providing our feedback.

Risk management and technology governance are two particular areas of focus for Governance Institute. We made a submission on the consultation leading to the development of the recently released 2020 Cyber Security Strategy. In our submission we recommended that cyber security be seen as a *whole-of-business* risk management issue and should be a standing agenda item for organisations' governance committees. We have also developed a range of resources to assist our members and others understand key risk and technology governance issues.

We welcome the opportunity to comment on the Consultation Paper – *Protecting Critical Infrastructure and Systems of National Importance* (Paper).

General comments

Governance Institute supports the expansion of the definition and scope of critical infrastructure and developing an enhanced framework to ensure the security and resilience of Australia's critical infrastructure.

Governance Institute recommends:

- Where possible, existing roles, frameworks and data flows for emergency management, both at the state and federal level, should be leveraged to increase efficiency. Similarly, where there are existing nominated hazard leaders and hazard types in various jurisdictions, these should be leveraged and any relevant new ones identified or nominated to enable maximum cooperation and efficiency. Examples of areas where existing roles could be leveraged include flood, biosecurity, health and fire hazards. Recent events have clearly demonstrated that groups working cooperatively with the benefit of good data and information can achieve more in an emergency, than a series of poorly informed disconnected initiatives.

- There should be an explicit focus in the definition of critical infrastructure not only on tangible, physical assets such as roads, railways and airports but also on nationally important *data* systems that are either key to economic activity (such as the Australian Securities Exchange and other exchanges) or which provide critical data to relevant core sectors such as the Bureau of Meteorology (BoM).
- Where a positive role and responsibility is identified, that this is supported by clearly articulated expectations, relevant minimum standards and training to ensure smooth operations in the case of an emergency.
- Any new framework needs to have clear, integrated and consistent governance and reporting, as well as a nationally consistent and transparent risk assessment and management approach.
- Communication and training, as well as a way to assess the integrity and authenticity of that communication, will be important components of implementation, to ensure that all involved in the protection of critical infrastructure understand their obligations, the relevant processes and reporting arrangements
- Where obligations are imposed on organisations, there needs to be an appropriate balance struck to ensure there is not an increased regulatory burden or unnecessary ‘red tape’.

Responses to specific questions

We have not provided answers to all of the questions in the Paper but have provided comments on issues of key importance to our members.

1. Do the sectors above capture the functions that are vital to Australia’s economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

We propose that sectors should be considered based on their contribution to national productivity. On this basis we consider that natural and significant natural heritage assets are also possible inclusions, given their social and cultural significance and their value related to tourism given it is a significant sector of the economy.[1] In this context manufacturing may also be relevant, given how we have seen this sector pivot during COVID-19 to produce sanitising gel and personal protective equipment supporting emergency efforts. It will be important to note that changing contexts will impact on industries and sectors at risk. For example, international supply chain disruption have brought into the spotlight key dependencies in agriculture, construction and other trade-exposed sectors. We also note that government is not explicitly included as a sector.

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

The focus of the current definition appears to be primarily on *physical* assets. Given the increasing importance of data assets to organisations in all sectors, we suggest the definition is broadened to explicitly encompass *critical information* infrastructure such as stock exchanges, payments systems, property registers or core spatial data systems. We note that the European

[1] We note this sector has been severely impacted by the pandemic but will recover.

Union (EU) distinguishes between critical infrastructure and critical *information* infrastructure.[2] Outsourced and cloud arrangements for relevant data systems also need to be captured to ensure that the jurisdiction in which they are located and the availability arrangements or risks are clearly understood.

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

An important factor to consider under this heading is the need for a nationally consistent hazard and risk assessment framework to ensure consistent risk rating as well as alignment and an integrated system of risks and controls. Given the learnings from COVID-19, a degree of *supply chain analysis*, for example, outsourced hosting arrangements for data, and also *compound risk* (one infrastructure affecting the operation of several others, for instance telecommunications) should also be considered.

4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?

Our members work in a range of organisations and industries, so it is difficult to generalise, but hazards would include: climate change, water scarcity or disruption of water supply, natural disasters (flood, fire, storms), disruption of communications, transport or electricity, pandemics, including various types of influenza.[3], cyber-attacks (these have increased dramatically during COVID-19). Threats may also include some types of digital disruption, for instance the use of social media to spread unsubstantiated or intentionally misleading information of influence democratic processes or intentional or unintentional effects of the use of Artificial Intelligence (AI) As an organisation focused on good risk management, we note there may also be a need and an opportunity to safeguard the significant amount of innovation, innovation capability and intellectual property developed in Australia each year.

The threat landscape is increasing in scope and complexity and there are more ‘external’, global or complex risks requiring organisations to increasingly integrate proactive and agile risk management into their governance structures. The Governance Institute strongly supports the importance of a strong organisational risk culture and an enterprise-wide and pro-active risk approach as part of an organisations’ governance framework.[4]

5. How should criticality be assessed to ensure the most important entities are covered by the framework?

In practical terms, we suggest that dependency mapping in consultation with relevant infrastructure owners may be the easiest way to assess criticality, as it may be easier for organisations to identify their input supply chain than their output dependent (downstream)

[2] To reduce the vulnerabilities of critical infrastructures, the European Commission introduced the European Programme for Critical Infrastructure Protection (EPCIP). This is a package of measures aimed at improving the protection of critical infrastructure in Europe, across all EU States and in all relevant sectors of economic activity. The EU initiative on Critical Information Infrastructure Protection (CIIP) aims to strengthen the security and resilience of vital Information and Communication Technology infrastructures

[3] The EU has also identified weather in space as a potential risk given the possibility of damage to communications infrastructure from solar flares. Given the significant increase in the amount of communications infrastructure being deployed in space, the risk of compound collisions and debris damage to Australian and indeed global communications networks is also possible and the damage to important communications infrastructure could lead to significant disruption.

[4] See Managing Culture: A good practice guide, Governance Institute of Australia, 2017.

supply chains. Spatial mapping may also be helpful, as it will serve to visualise any proximity related issues or dependencies that may not otherwise be visible.

It may also be useful to look at how this issue has been addressed in overseas jurisdictions, for example, the EU.[5]

6. Which entities would you expect to be owners and operators of systems of national significance?

We consider that the owners and operators of systems of national significance will include: government entities, in particular key data providers such as BoM whose data informs the operation of many other sectors such as transport, aviation, defence, water and agriculture. Media and social media platforms and their integrity also need to be considered given the increasing role they play as sources of information for individuals and businesses.

Similarly, stock and other exchanges and payment systems, electricity providers, transport infrastructure providers, telecommunications infrastructure providers and water infrastructure providers and their data systems will form part of the wider scope.

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?
8. What might this new TISN model look like, and what entities should be included?

Our members consider that a revised TISN would support the reforms outlined by continuing to provide a forum for communication, collaboration and information exchange.

It will be important to identify relevant standards to guide the development training program. A significant and secure online presence and resources to support real-time data flows and the exchange of information during emergencies is also important to consider.

Notably, any system and data collection used to collate relevant data from critical infrastructure owners and operators as well as systems developed to communicate threats would, in themselves, become critical infrastructure.

An example of how this may work is the implementation of the *Water Act 2007* (Cwlth), which established BoM as the coordinating agency for water information from both public and private sectors nationally. Implementation of the new data collection and reporting role of the Bureau included the establishment of both jurisdictional and national coordinating committees, the development of data standards, the provision of training and the provision of funding to support implementation and expand data coverage, where required.

Learnings from BoM on this multi-year journey may be useful to inform the implementation of this initiative and some of the systems developed may also form part of its data infrastructure.

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

Government could support critical infrastructure entities by:

- developing a map of interdependencies in consultation with sector representatives

[5] The EU EU has the assessment framework Geospatial risk and resilience assessment platform (GRRASP) – refer https://ec.europa.eu/jrc/en/scientific-tool/geospatial-risk-and-resilience-assessment-platform. .

- developing a nationally consistent risk assessment and reporting framework, consistent terminology and clear minimum expectations and requirements
- considering whether to require these entities to have a security plan, similar to the model of the *Protective Security Policy Framework* and the EU requirements
- providing training, market intelligence and communication channels, and
- identifying clear reporting and escalation processes.

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

Our members consider that addressing security risk also encompasses communication, reporting and escalation as well as the development of a risk and cyber security aware culture within organisations. An enterprise wide approach to governance, risk management including cyber security is key.

Governance Institute's recent Risk Management Survey identified inadequate reporting on risk as a key pain point. We consider that there is likely to be a need for real-time data and the ability to report in real time including information to location-based analysis and intelligence. Where possible we suggest leveraging existing government registers and systems, such as the BoM data and contextual data systems or the spatial data collections of Geoscience Australia, which already have national coverage. These government entities may also provide existing contextual data to enable modelling of incidents and response requirements and logistics.

As noted above, we consider appropriate training and development and the identification of clear roles and processes will be critical to success. A suitable existing framework and communication mechanism that should be leveraged is the PPRR approach used in the emergency services sector - planning, preparedness, response, recovery.

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

An approach to consider would be to provide national minimum guidance with sectoral 'best practice' models – the Essential Eight for cyber security is a useful precedent.

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

Given our comments in 9 above about the need for nationally consistent minimum requirements and standards there will be a need to find a balance between customisation for the needs of specific sectors and the need for integrated reporting. It will be important to automate data flows and existing processes and obligations to the maximum extent possible, both to reduce manual burden and to increase the timeliness of a response.

17. 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?

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

Any approach to regulation will need to be multi-faceted involving a combination of approaches: 'black-letter' law, industry standards (local and international), inter-governmental and industry codes. It will be critical for the Australian Government and existing regulators to work cooperatively with other governments and each other in this area. Any regulatory framework should also allow for electronic reporting and the provision of real-time data.

A useful example for regulators of an agency and its experience with a range of additional responsibilities is BoM which gained a water information role under the *Water Act 2007* (Cwlth) – see 7 above. The Bureau's learnings and those of other agencies involved in similar initiatives could be incorporated into the development and implementation of this, much wider, national framework.

19. How can Government better support critical infrastructure entities in managing their security risks?

Our members consider that Government can better support critical infrastructure entities to manage these risks through co-design, providing information, notifications, training, support and information networks and appropriate funding.[6] It is also likely that Government itself may indeed be a critical infrastructure provider. It therefore it may be useful to establish the opportunity for existing and new critical infrastructure providers to develop networking and mentoring relationships to accelerate maturity across the sectors.

If you have any questions concerning this submission or would like to discuss any aspect please contact our General Manager, Policy and Advocacy, Catherine Maxwell.

Yours sincerely

[redacted]

Megan Motto
CEO

[6] On the issue of funding see our submission *Australia's Cyber Security Strategy 2020: A call for views*.