Government of South Australia
Department of the Premier and Cabinet

Response to the Australian Government's consultation paper: Protecting Critical Infrastructure and Systems of National Significance

September 2020

Introduction

The Department of the Premier and Cabinet (DPC), in collaboration with other South Australian Government departments, submits this high-level response to the discussion paper, noting additional information provided during meetings and forums.

South Australia is committed to protecting the critical infrastructure and systems that underpin and enable our everyday social and economic activity. It is important these remain operational in the face of different hazards and can withstand increasing and sustained threats, particularly cyber-attacks.

The national and global threat and hazard environment – both natural and man-made – is changing rapidly and becoming increasingly more complex. Whilst our increased use of cyber technology creates commercial, economic, social and technological opportunities, it also creates new avenues for malicious actors and actions inconsistent with state and national interests.

Ensuring reasonable and proportionate steps are taken to protect critical infrastructure and systems from the risks of sabotage, interference, espionage and coercion, and increase resilience to all hazards is a shared responsibility. The Department supports the intent of the framework as it is understood – to protect Australia's critical infrastructure from all hazards in an increasingly complex hazard environment and support entities responsible for assets and systems of national significance in uplifting protective and resilience measures. It is, however, important to balance strengthening protective arrangements with enabling economic and sectoral growth and investment.

It is recognised that the new framework proposed by the Australian Government, and the associated legislation, will enhance the suite of measures already in place. It is understood that the proposed legislation will expand the scope, remit and obligations imposed on entities through the *Security of Critical Infrastructure Act 2018* (SoCI Act). Noting the Act's current safeguards, concerns about the Commonwealth's ability to direct the states and territories and their instrumentalities remain.

Whilst recognising the intent to build on existing regulatory activities wherever possible, this framework should not overly complicate the existing regulatory requirements for those

entities – both state and privately owned and operated – that will fall within the new thresholds.

The proposed risk-based approach will require a shared understanding of the threat context and the ability to quickly share information and intelligence during events and incidents. States and territories are responsible for managing emergencies within their borders, and how this framework interacts with the existing 'all hazards' emergency management arrangements and risk reduction requirements requires consideration.

It is timely for national governance arrangements which support government decision making and collaboration with industry to be reviewed and enhanced. The DPC, with other partner government departments, will continue to be a cooperative participant in these networks and governance fora.

This response draws out concerns and suggests areas that require further exploration. More detailed input on issues and opportunities will be given once more detail, including the draft Bill, becomes available. The DPC would welcome the opportunity to review the draft Bill and participate in further consultation, potentially through an appropriate Parliamentary Joint Committee process, before the legislation is passed.

Strategic connections

Efforts to enhance protection and resilience of critical infrastructure and significant systems are inherently linked to protective security and cyber security activities with the outcomes of each contributing to strong security culture, practice and systems.

While there is a strong focus on cyber security, the reference to managing 'all hazards' risks significantly broadens the scope of the framework and obligations on entities, depending on how this is referenced in the Bill. Further clarification on expectations is required noting the significant and long-term investments that could be required to enhance resilience against all natural and man-made disasters for critical infrastructure and systems, particularly physical assets and networks. This discussion should be guided by existing national frameworks such as the National Disaster Risk Reduction Framework.

It is noted the Foreign Investment Review Board approvals processes is linked to the SoCI Act. As such, the potential impact on the National Security Test proposed under the *Foreign Acquisitions and Takeovers Act 1975* should be further explored. If the National Security Test adopts the definitions and thresholds proposed through this reform, the scope of that test will change adding a layer of complexity to the foreign investment approvals regime beyond the scope of the previous consultation.

Information sharing is fundamental to supporting a shared understanding of risk, decision making during events, and ensuring suitable transparency of decision making particularly with regards to the powers of direction and declaration of assets. Consideration must be given to how the Australian Government will share information with industry members, as well as states and territories appropriately and in a timely manner. A formalised approach to how information is shared, such as the Defence Industry Security Program model, should be considered. Resolving the Intergovernmental Agreement on Information Sharing may also help strengthen information sharing between the Commonwealth, state and territory Governments.

Definition and scope

The current definition of critical infrastructure is, '*those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social and economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security*'.

This definition remains mostly appropriate, particularly in the context of a national framework. However, it may be beneficial to reference the system created by physical facilities, supply chains, information technologies and communication networks, noting that impact onto singular elements can often be mitigated or managed through continuity arrangements. Criticality should also be assessed in relation to the impact on the nation.

The industries included in the framework are appropriate noting this means some sectors already involved in the Trusted Information Sharing Networks (TISNs) and Critical Infrastructure Advisory Council (CIAC) may become subject to the legislation. Ongoing industry collaboration will be required to build mutual understanding, consider how obligations are interpreted and operationalised, and navigate requirements.

Given the interconnectivity between key sectors, and the variety of entities involved in supply chains, clarification about how this definition is applied in different contexts, particularly in the regulatory and operational sense, should be sought. The term 'critical infrastructure' is used quite broadly, often with different definitions, perspectives (national, state and local) and understanding which can be confusing.

To this end, articulating 'categories' in the framework is welcome as it reflects the intention to focus increased and proportional obligations based on criticality and risk from the national perspective. However, it is important that the system does not become overly complex for entities to engage with and information is shared between the Australian Government and entities about risk assessments and reasoning for how they are categorised.

Positive Security Obligations and Regulatory arrangements

The principles articulated in the discussion paper are broadly supported, however the use of such broad principles and language creates a risk for legislation (and associated powers) to be applied more broadly in the future and in a manner that does not align with the current stated intent.

Categorising security obligations under three domains (physical, cyber and personnel) aligns with the South Australia Government's existing protective security policy. While it is understood the Australian Government has proposed broad principles to enable all aspects of security risk to be considered, further detail and specificity is required to ensure entities can prioritise investment and effort to achieve objectives. To this end, the principles could also incorporate a focus on managing the impacts and consequences of disruptions or failures as these remain relatively consistent across the variety of threats and hazards.

Significant ongoing consultation and time will be needed to develop the supporting regulations. Furthermore, South Australia is cautious about increasing regulatory obligations that do not deliver material benefit to the nation, industry and society or that do not balance the importance of protecting the national interest and sovereignty with opportunities for economic development, industry investment, innovation and expansion into the future.

The question of who will act as the regulator requires further consideration, and we have not been able to fully consider whether any existing South Australia Government regulatory teams could contribute given the short timeframes and limited detail currently available. The potential conflicts between national and state-based regimes and requirements must also be resolved. All existing regulators (State Government or otherwise) would need the detail of the regulations to consider the skills and resources required to expand their existing service to accommodate these requirements on behalf of the Commonwealth and further negotiations would be required to consider a variety of operational and accountability matters and funding arrangements.

The commitment to providing education, awareness and guidance programs is supported as a foundational element of enhancing security and building mutual understanding of contemporary and emerging issues.

Enhanced Cyber Security Obligations & Opportunities for Cyber Assistance

South Australia Government agencies are mandated to comply with the SA Protective Security Framework (SAPSF) which includes the SA Cyber Security Framework (SACSF). Any new reforms, such as those proposed, should have regard to existing policies and standards – particularly in instances where they are already ensuring effective management of cyber security. Detailed mapping is required to understand where there may be additional financial costs and duplication associated with the new obligations. Pending further detail, there is a concern that additional or duplicative policy instruments could impose a time and/or financial burden, with limited obvious benefit over and above the work already underway.

In South Australia, as in many other jurisdictions, cyber incidents are recognised under the state emergency management arrangements. In South Australia, government agencies are obligated to report incidents to the DPC, as Control Agency for cyber security, to feed this information into emergency management considerations. DPC would not support any obligation or process that sees government agencies either bypass current reporting obligations within the state and/or results in some entities being required to report twice under different reporting regimes.

States and territories are responsible for responding to and managing emergencies within their borders. There has been a long-held practice of states and territories leading response to major cyber incidents within their jurisdictions (typically for government agencies and assets) and then seeking assistance from the Australian Cyber Security Centre (ACSC) if required. This system is working effectively, and there is no benefit to be gained in changing this approach, particularly when dealing with cyber security matters in government agencies. Any reporting obligations for government entities should have regard to the pre-existing Cyber Incident Management Arrangements for Australian Governments (CIMA). The CIMA is currently functioning as intended and providing an excellent level of coordination and collaboration around cyber incident response, whilst still providing the opportunity for each state and territory to tailor the response measures to their specific case. Under the current CIMA model, the ACSC are still able to provide considerable technical and incident response assistance, if required, and on request.

Government and Industry collaboration and governance

Collaboration between government and industry is critical to connect the expertise and capability required to increase the resilience and security of our most critical systems.

The opportunity to enhance the national governance and collaboration arrangements is welcomed, and consideration should be given to how the TISNs and CIAC are constituted.

The role of the CIAC and its relationship to other peak national committees such as the Australia New Zealand Emergency Management Committee and Australia New Zealand Counter Terrorism Committee should be clarified to ensure connected strategic directions and intent. The role of the TISNs during emergency response might also be considered. It is noted this should be informed by potential recommendations emerging from other investigations such as the Royal Commission into the National Natural Disaster Arrangements.

The approach to future strategies and activities could be reconfigured to focus on connectivity and interdependency and how common risk and consequences are mitigated/managed. Prioritising effort and establishing common focus across sectors, and exploring connections to other strategic partners, to address highest risks or vulnerabilities would deliver system wide benefits.

Framework and legislation development process

DPC understands the draft Bill is intended to expand the existing SoCI Act and will be focused on setting principles and objectives to achieve the desired outcomes. Further it is understood that regulations will be developed for each sector through a collaborative process. It is acknowledged that this approach will enable the unique and specific circumstances and vulnerabilities of each sector to be considered, including how they connect with, rely on and enable other sectors across the broader national architecture.

However, it is not possible to provide fully considered comment without the draft Bill and the draft regulations which will detail how the legislation will be operationalised and expectations for how entities will meet the objectives and positive security obligations. DPC would welcome the opportunity to provide further input through an additional process such as a referral to an appropriate Parliamentary Joint Committee.

A suitable ‘grace period’ is supported to ensure sufficient time is provided for the regulations to be developed and entities to understand new obligations and requirements before any future legislation takes effect.

While it will be important for entities to achieve identified minimum standards and requirements within an appropriate timeframe to deliver genuinely system-wide benefits, a progressive improvement approach should be adopted given the potential costs and operational changes this could place on some entities. To this end, investment in ongoing education and awareness programs, as well as opportunities for public-private partnerships to enhance collective protections and resilience should be explored.

Furthermore, existing risk assessment, criticality guidelines and interdependency mapping tools and processes should be used to avoid complexity and harness existing knowledge.

South Australian Government as a critical infrastructure and system owner/operator

Noting the thresholds are yet to be finalised, it is anticipated that some South Australia Government assets and systems will fall within the remit of the proposed legislation and be subject to the obligations and responsibilities outlined. At this time these primarily relate to health and public transport services, however, urgent clarity on the thresholds is required to fully assess the impact on critical infrastructure and systems in which South Australia has an interest.

Clarification is also required about how critical infrastructure already captured by SoCI Act will be impacted.

Notwithstanding the safeguards within the existing SoCI Act and the shared commitment to enhance national, cyber and protective security, constitutional concerns associated with the existing Ministerial powers of direction remain particularly noting the broader application of the legislation.

South Australia is enhancing protective measures through:

- The new SAPSF which establishes information, personnel and physical security requirements which each department must apply based on their risk and operating context, which will be supported by a security maturity assessment model that will identify and assure progressive improvements.
- The mandatory cyber incident reporting and cyber security protections outlined in the SACSF, (which forms part of the SAPSF requirements).
- Physical security requirements for critical infrastructure identified as site of significance to the State.

It was encouraging that the Australian Government displayed willingness to consider how these existing policies, which share the objectives of the proposed framework, can meet proposed obligations. DPC welcomes this approach, and will seek to have these, and other existing licensing and accreditation requirements, formally recognised through regulations and policy.