ACT Justice and Community Safety Directorate

Comments on the Australian Government's
Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

Note: On 11 September 2020 the ACT Government assumed a Caretaker role ahead of the ACT election on 17 October 2020. These comments are provided by the Justice and Community Safety Directorate (Directorate) and are made in accordance with the ACT's Caretaker Conventions. The comments provided by the Directorate in this paper should not be taken as the views of the ACT Government and may be subject to change.

Directorate Contact

Security and Emergency Management Branch

Justice and Community Safety Directorate

T. 13 22 81

Introduction

On 12 August 2020 the Minister for Home Affairs announced the release by the Australian Government of the *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* (Paper).

The Paper describes the Australian Government's decision to introduce reforms to strengthen the security and resilience of Australia's critical infrastructure. The reforms are proposed to include:

- a security obligation for critical infrastructure entities;
- enhanced cyber security obligations for entities most important to the nation; and
- Government assistance to critical infrastructure in response to significant malicious cyber activity.

The Australian Government has sought feedback on the Paper from governments, business, industry and the critical infrastructure sector in the following areas:

a. the sectors that capture the functions vital to Australia's economy, security and sovereignty and nationally significant systems;

b. how the government supports critical infrastructure to manage risks, particularly cross-sector dependencies;

c. what sectors are subject to security obligations and its associated costs;

d. how regulation will occur and the role of sector regulations to support entities in meeting their security obligations; and

e. what organisations should undertake a security-related regulatory role and the support required.

The Directorates acknowledge the focus and investment of the Australian Government to increase the protection of critical infrastructure and systems of national significance. The Directorate offers the following comments on the consultation paper and associated matters.

Description	Comments
General Observations	
Requirement for the enhanced critical infrastructure framework	The Directorate recognises the intent of the reforms and the proposed framework as an initiative under *Australia's Cyber Security Strategy 2020*. The Directorate acknowledges the need to strengthen the protection of critical infrastructure and systems of national significance across Australia in response to the elevated security threat environment. A disruption of Australia's critical infrastructure has the potential to significantly compromise the supply of essential services across Australia. With increased threats to cyber security, the proposed framework will build on the existing requirements under the *Security of Critical Infrastructure Act 2018* (SOCI Act) and develop an enhanced cyber security capability for the nation's critical infrastructure sectors. The Directorate notes that there was no opportunity for states and territories to participate in the early preparation of the framework. Improved results in the future stage of this project may be achieved through enhancing the governance arrangements, including a high-level consultative group particularly as the development of the Bill progresses.
Timeframes for review and consultation	Whilst the Consultation Paper recognises that "prompt action is required to ensure Australia is in a strong position to address all threat to our critical infrastructure" the timeframes to achieve legislative reform and adequately consult on the proposed changes (including the draft Bill) appear very limited. The Directorate is concerned that there may not be an appropriate opportunity for the Australian Government to consult on the draft legislation before it is introduced into Parliament.
Scope and entities captured	The consultation paper identifies the sectors to which the additional measures will apply however the thresholds are still being developed and refined. The Directorate encourages the ongoing consultation by the Australian Government on this matter. It will also be important for all governments to map out each of the sectors to clearly identify entities that will fall under the definition of a 'Critical Infrastructure' entity or those defined as a 'System of National Significance'. The Directorate suggests that this piece of work is undertaken as a matter of urgency and prior to any introduction of legislation.

	The Directorate recommends that the Australian Government consider the application of the proposed framework to the manufacturing sector which may hold intellectual property or products that is critical to Australia's security.
Commonwealth consultation and engagement with states and territories	The Directorate acknowledges the effort of the Australian Government to brief and consult with governments, business and industry about the reforms and providing comment on the consultation paper. The Directorate notes the ambitious timeframes for briefings and consultation. This is occurring at a time of significant competing pressures including managing the COVID-19 pandemic, providing input into the *Royal Commission into National Natural Disaster Arrangements* and preparing for the natural disaster season. These conflicting priorities have impacted on the ability of stakeholders to provide comprehensive comment and fully engage in future stages or the reforms. The Directorate views that the Australian Government should not consider the consultation phase to be a one-off. The implications of the new framework and the amended SOCI Act are considerable. It will be important that the Australian Governments seeks to consult as much as possible about the reforms and the legislative amendments, particularly as further details are known. The Directorate is concerned that opportunities for the Australian Government to consult and seek feedback on the legislation appear to be very limited. This may result in lost opportunities, difficulties in interpretation, challenges with long-term regulation and reducing a fit for purpose model. The Directorate would prefer to work with the Australian Government and other states and the territories to review and comment on the legislation before it is introduced into Parliament. This will help to better target the framework's intent and ensure that it can be effectively implemented.
Cost of reform and regulation	The Directorate acknowledges that the positive security obligations, and the enhanced cyber security obligations will require additional investment by critical infrastructure owners including governments. The Directorate queries whether the Australian Government has modelled the cost to critical infrastructure owners and operators to comply with the proposed reforms. Introducing policy reforms or new legislation without clearly understanding the impacts is likely to result in unintended consequences, including the potential that compliance is inhibited by cost.

All-hazards approach	The purpose and objectives of the framework needs further clarification and strengthening. The Overview of the framework discusses the range of hazards that may compromise Australia's critical infrastructure. These hazards include physical, personnel, cyber security and natural disasters. The framework also states that an all hazard approach will be taken to protect critical infrastructure. All-hazards is a term typically used in emergency management and is normally associated with natural hazards (such as storms, floods and bushfires). The features of the enhanced framework (positive security obligation, enhanced cyber security obligation and government assistance) all relate to security matters and not natural disasters. Is it the intention of the framework to enhance the resilience of critical infrastructure to natural disasters? If so, the features of the enhanced framework appear limited in relation to natural disaster resilience. Noting that security threats appears to be the highest-level risk, focusing on natural disaster risks may unnecessarily increase the cost and complexity of the reforms.
Visibility of legislative reforms	The Directorate notes that the Bill to amend the SOCI Act is being drafted. The Directorate recommends that the Australian Government makes a draft of the Bill available to states and territories for review and comment prior to its introduction into Parliament. This will support the understanding of the application of the reforms in a practical and operational sense, and the potential cost and resource implications.
Implementation and ongoing regulation of reforms	Collaborating on the options and preferred approaches to the regulation of the new reforms will be a critical part of the reforms and ensuring there is no duplication of effort that is already applied under current state based regulatory frameworks. The Directorate views that it would be in the interests of the reforms for the Australian Government to undertake a deep-dive mapping exercise of existing regulatory mechanisms to ensure that these are clearly understood. The Directorate notes in the consultation that the Australian Government will work with critical infrastructure entities to ensure that these reforms are developed and implemented in a manner that secures appropriate outcomes without imposing unnecessary or disproportionate regulatory burden. This will be in accordance with guidance from the Department of the Prime Minister and Cabinet's Office of Best Practice Regulation.

	This is equally important for governments to ensuring there is no duplication of regulation which would have a significant impact on government resources and associated costs. It would also be appropriate to further understand the proposed roles and responsibilities of the regulators to determine where the ongoing regulation of the reforms best fit.
Financial implications	The Directorate notes that the Australian Government has indicated that there will be no financial assistance available to sectors to comply with the requirements of the framework. The Directorate views that there could be a significant financial cost to entities that are captured by the amended legislation. This aspect will need to be considered at all stages in the design of the new framework and made as efficient and low cost as possible.
Thresholds (transport and education)	The Directorate encourages the Australian Government to continue to consult extensively in the design of the new thresholds. The Directorate is supportive of the proposed thresholds for transport. It is unclear if the definition and thresholds for the education sector will include primary, secondary and vocational institutions.
Principle-based Outcomes	The Directorate is supportive of the intent to move towards a principle-based approach to managing Positive Security Obligations (PSO) and considers it necessary to taking a proactive step in strengthening cyber security measures in the current environment. It will be necessary to further draw out the details of the PSO and potential implications on each of the sectors.
Resourcing for TISN	The Directorate notes the vital importance of information sharing between governments, business and industry and the proposed role of the TSN to facilitate this. The Directorate notes the intention of the Australian Government to strengthen the TISN arrangements. It will be critical that the Australian Government identify and effectively resource this requirement to sustain an active TISN noting its primary role as the information sharing mechanism.
Preparatory activities and Playbook	The consultation paper indicates that ***Government*** will work with owners and operators of systems of national significance to build their cyber security capability and understanding of threats to their business through participation in 'preparatory activities', including cyber security activities and the development of playbooks.

	The Directorate assumes that the Australian Government will lead this work.
Limitations on Government Directions	The Directorate views that careful consideration will need to be given to establishing appropriate checks and balances in any mechanisms/processes intended to give the Australian Government statutory powers to give directions to entities to act in response to a cyber threat. Such an approach. It may be suitable for the Australian Government to give general directions about cyber security enhancement. However, if the directions are likely to be coercive in nature or impact on the operations of the business, the approach should provide mechanisms for the entity to have their position or actions independently considered.