The Australian Industry Group
Level 2, 441 St Kilda Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 3004
Australia
ABN 76 369 958 788

15 September 2020

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

Dear Sir/Madam

PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE CONSULTATION PAPER

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Department of Home Affairs on its consultation on reforms discussed in its *Protecting Critical Infrastructure and Systems of National Significance* Consultation Paper. Our members are businesses of all sizes and many sectors across Australia. As shown with COVID-19, many of these businesses are essential, contribute to our economy and form critical parts of supply chains and critical infrastructure.

Overall, we support measures to improve the security and resilience of our critical infrastructure, with non-regulatory approaches as the default response before contemplating heavier forms of regulation. However, we consider further time will be required to properly consult on any proposed legislative reform and recommendations arising from this consultation. For instance, details currently remain unclear on the nature of the reforms including its scope, definitions, measures and cost-benefit impact. This is especially critical in light of the wide breadth of sectors that could be captured by these reforms and the impact of the current COVID-19 pandemic on businesses and the community.

We welcome being included as part of further consultations, and bringing in relevant members covering a wide range of sectors that may be captured by these reforms. We would also welcome the opportunity to work closely with the Department of Home Affairs as the consultation progresses.

In the meantime, we would like to provide preliminary views. As further consultation is undertaken, there may be additional matters raised.

1. Consultation process

We welcome the consultative approach that the Department has undertaken in holding virtual town halls and industry specific workshops. We encourage that this level of stakeholder engagement continues for the remainder of the consultation process.

To ensure that proper consultation be undertaken for any proposed reforms, there should be proper assessment of issues and underlying causes that the reforms are seeking to specifically address, options to address those issues and causes, and proper cost-benefit assessment of any proposed reforms.

While the Consultation Paper provides a high level overview of the proposed reforms, relevant details to enable adequate stakeholder scrutiny remain unclear and warrant further development and consultation. These considerations should not be rushed and require sufficient time to work through in consultation with relevant stakeholders to ensure appropriate measures are put in place. This is especially important in light of the wide breadth of sectors that could be captured by these reforms and the current COVID-19 pandemic.

For instance, if legislative amendments are proposed, we strongly recommend that an additional stage with adequate time for consultation with relevant stakeholders will be required including a Draft Report and an Exposure Draft Bill. However, with the tight timeframe set by Government for this consultation process, we are unsure if this will be achievable and recommend that time be extended for this consultation process.

We are also mindful of the risks of unintended consequences for businesses and the community arising from rushed legislative decisions with limited consultation, as seen with the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act). In contrast, when the Telecommunication Sector Security Reform (TSSR) was developed for the telecommunications industry as part of the critical infrastructure security regime, this took several years of negotiation and collaboration between Government and industry before a more workable version was implemented.

2. Scope and definitions (Consultation Paper Questions 1-6)

Critical infrastructure is currently defined in the current Australian Government's Critical Infrastructure Resilience Strategy as "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 or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security". In accordance with the *Security of Critical Infrastructure Act 2018* (Cth) (SCIA), this currently places regulatory obligations on specific entities in the electricity, gas, water and maritime ports sectors. The Consultation Paper proposes to introduce new security obligations for critical infrastructure entities and expand the scope to a broader range of sectors (i.e. banking and finance; communications; data and the cloud; defence industry; education, research and innovation; energy; food and grocery; health; space; transport; and water).

The scope of companies affected by this consultation is a major question. The following should be factored in when considering the scope of companies that are proposed to be captured by these reforms:

- As shown with COVID-19, many businesses across many sectors are essential, contribute to our economy and form critical parts of supply chains and critical infrastructure and systems.

- With more connectivity enabled through emerging technologies such as the Internet of Things (IoT) and equipment supplied to provide essential services, there may be difficulty in defining the boundary line between critical and non-critical infrastructure and systems.

- Some businesses service and supply to multiple sectors – some of these sectors are proposed to be covered under these reforms. For example, in the case of "data and the cloud", this can be interpreted to be overly broad in meaning – it could apply to almost any business with an online platform or presence and can operate across sectors. There will need to be more specificity to properly define this sector, and potentially other sectors too. Otherwise, this can create a disproportionately greater regulatory burden for businesses that have more diversified portfolios and operate across sectors.

- Creating new requirements for sectors including suppliers and manufacturers that operate across sectors and are not historically subject to the critical infrastructure security regime also present a disproportionate regulatory burden for those businesses.

- Some businesses may be more mature and familiar with their security requirements due to the nature of their industry; for example, those sectors currently subject to the critical infrastructure security regime, and sectors that have a high level of engagement between Government and industry such as the defence industry.

- Technological solutions such as remote monitoring are available to support critical infrastructure owners and operators that deploy sophisticated assets.[1] Such sophisticated assets can come from many markets (domestic and overseas), and diagnostics centres associated with them may be located offshore. Permanent remote monitoring solutions should be allowed under an established process e.g. through approved IT hardware and software connection practices, international cyber security standards and practices, and approved data sets allowed to be transferred offshore subject to appropriate data protection requirements.

[1] Applications of remote monitoring may include: monitoring the performance of the asset against expectations; identifying premature degradation which would benefit from intervention before it leads to failure; collecting information across the installed base to gain insights for improvement of operational practices; identifying equipment or subsystem failure and despatching of spare parts or specialist offshore personnel; patching of firmware or software for performance and security reasons including cyber security; and remote training and overseeing operator activities where overseas expertise can assist.

- Associated with the scope of businesses covered, definitions under these reforms and referred to in the Consultation Paper will require further clarification, including: “national significance”, “systems of national significance”, “critical”, “criticality”, “critical capability”, “critical infrastructure assets”, and “government assistance”. Providing examples of the types of companies and definitions (as referred to in these reforms) in relevant legislative instruments will also help to provide better clarity on the scope.

Therefore, taking an “economy-wide” approach to this legislation is fraught with challenges and risks, with the potential for creating unintended consequences and unnecessary regulatory burden. We recommend the following actions be further undertaken to help alleviate those concerns as part of this consultation:

- Proper assessment and careful consultation on a sector-by-sector basis, with all relevant stakeholders.

- Given the wide sectors that have been identified, we suggest an incremental approach to reviewing each sector to ensure unique requirements for each sector are properly understood and assessed.

- As mentioned above, further consultations should include sufficient time for an additional stage to adequately consult with relevant stakeholders on a Draft Report and an Exposure Draft Bill (if legislative reform is recommended).

- The Government will need to be mindful of the web of national security and regulatory legislation that connects to the SCIA. The Government’s currently proposed changes to the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (FATA) would subject any business responsible for, or with a significant stake in, critical infrastructure covered by the SCIA to substantial new obligations and powers under the FATA. Thus decisions about the scope of the SCIA will have larger implications that need to be fully considered in regulatory impact analysis.

3. Government-Critical Infrastructure collaboration to support uplift (Consultation Paper Questions 7-9)

The Consultation Paper discusses collaboration between Government and critical infrastructure entities, and seeking to enhance and integrate Government’s existing critical infrastructure education, communication and engagement activities, through a reinvigorated Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) and updated Critical Infrastructure Resilience Strategy.

Overall, we would support non-regulatory approaches as the default response before contemplating heavy-handed regulation e.g. supporting the application of industry-led standards, education and training. We suggest other activities mentioned in the Consultation Paper that would be worth exploring include: threat assessments and briefings; individualised vulnerability assessments; enhancing research, analysis and evaluation capabilities; and industry-government secondment program.

With respect to standards, there already exists standards and initiatives to support industry standards relevant to critical infrastructure and systems. Standards, if called up by regulation, offer a mechanism to quickly respond to changing markets. For example, Ai Group is involved in a partnership with the NSW Government, Standards Australia, AustCyber and other key industry stakeholders to harmonise cyber security standards across a number of key sectors. There is an opportunity for the scope of this work to be expanded to other sectors.

More generally, it is important that international standards are referred to as the baseline wherever possible. This will make it easier for Australian businesses to export their goods and services, as well as avoid the risk of creating domestic cyber security standards that creates a global competitive disadvantage for Australian businesses and barrier to investment in Australia. International agreements and requirements, and Australia’s regional market (import and export) may also influence the choice of standards. Associated with this, the Australian Government should continue to help fund Australian involvement in international standards development and it should ensure that an Australian filter (consistent with the WTO Technical Barriers to Trade provisions in Annexure 3) is applied before the adoption of international standards in Australia. This can be facilitated through a suitable forum such as Standards Australia to consider international standards discussions that impact on a wide range of sectors.

With respect to the Critical Infrastructure Resilience Strategy, we suggest improvements could be made in the following areas:

- Better alignment between Government departments, including DFAT, the Department of Home Affairs, Treasury and other Government agencies to drive improvements to more resilient infrastructure and national security protections.

- Collaboration between State and Federal Government departments and agencies. They all have an important role to play and removes duplication for participants.

With respect to the TISN, the following could be further explored:

- Jurisdictions being included in the TISN as the primary responders, which connects the Federal Government with industry in a much more meaningful and outcomes driven manner.

- Other sectors introduced in the TISN to create a more cross-functional and cross-sectoral representation of industry.

- Operationalising of segments or subgroups and functionally common informal networks in the TISN could enable greater agility and flexibility within the sectors.

- Prioritising flexibility within the TISN framework.

One of our members has previously participated in the Resilience Expert Advisory Group (REAG). They highlighted lessons learnt from the REAG workshops were that: state jurisdictions are a necessary key stakeholder within the TISN; and any future structure of the TISN should encompass not only the existing sectors, but individual segments within those sectors. They recommend supporting the ongoing work plan of the REAG, which is to continue mapping exercises in the State jurisdictions, facilitating ongoing learnings, and the collection of much deeper and richer data, whilst continually building on the ecosystem approach.

Another member considered that improvements could be made to the TISN to make it more relevant, given its large size. It suggested the ASD/ACSC's forums were very high value in terms of cyber security, and suggested more focus on these forums on cyber security and have this embedded in the TISN.

4. Initiative 1: Positive security obligations (PSO) – Principles-based outcomes, Security obligations and Regulators (Consultation Paper Questions 10-21)

The PSO initiative in the Consultation Paper proposes a set of principles-based outcomes across Australia's critical infrastructure sectors to protect entities from all hazards. Such obligations would then be set out in legislation for critical infrastructure entities to meet.

The Consultation Paper also raises questions relating to proposed security obligations and costs of compliance. And if new security obligations were to be imposed for a given sector, additional questions that arise relate to: whether there is a relevant and suitable regulator that should enforce compliance with these obligations for that sector; whether there are potential overlaps with existing regulators; and other regulator functions associated with cyber security e.g. education and guidance.

In general, we would support a principles-based outcomes approach in regulation, as it would be flexible enough to enable future proofing and therefore technology neutrality in a rapidly changing environment. However, this must be based on the threats faced by each industry, existing regimes and these will likely be different.

For instance, in the case of the defence industry, companies are expected to meet certain requirements when working in Defence projects, given the nature of its work. There are existing programs that may assist such as the Defence Industry Security Program (DISP), as well as international requirements such as managing controlled technology that may be subject to US export controls having extraterritorial reach (for instance, the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)).

With respect to the DISP, this is a membership-based program for the defence industry that includes requiring its members to comply with Defence's protective security policies, practices and procedures. DISP membership is encouraged, and in some cases, it is mandatory to join the program if businesses are doing sensitive or classified work. However, not every business has to have DISP membership to work in Defence. Nevertheless, any business that works in Defence and with industry should have appropriate security protections in place.

Another example is the energy industry. One member has suggested that existing regulators in the energy sector have not been favourable to increasing spending in cyber security, including the latest Australian Energy Regulator (AER) regulatory determinations for electricity distribution network businesses. It is unclear if this will change as a result of these critical infrastructure security reforms. However, it is clear that the current frameworks for assessing the costs and funding for cyber security for regulated entities in the energy sector is not aligned with increased cyber security capability. This will need to change if these reforms are to succeed.

For businesses that operate across sectors such as cloud service providers, it may be difficult to consider whether and which proposed principles-based outcomes and proposed measures should apply to them, without first understanding the various security requirements for each specific sector that they service. To help resolve this, a possible solution could be to undertake a thorough gap analysis and assessment of the proposed obligations against existing obligations across the various sectors in which these businesses operate. Once these are clarified for the various sectors, further consideration could be given to businesses that operate across sectors such as cloud service providers. And if it were to be deemed that a regulator is required to be appointed, the regulator will need to have the sufficient technical expertise to understand the complexity and nuances of cloud services, and the ongoing innovation and technology development in this space.

If a gap analysis and assessment of requirements for each specific sector were to be undertaken, we consider that further consultation will be required with relevant stakeholders. For instance, this may include: assessment of the level of maturity of practices; access to required standards and competencies to ensure vulnerabilities are identified, understood and risk controls put in place; readiness to be regulated; expected baseline competencies; and access to supported competencies training.

As mentioned above, we would be concerned about creating new security obligations (even if they are based on principles) without proper assessment of issues and underlying causes that the obligation is seeking to specifically address, options to address those issues and causes, and proper cost-benefit assessment of such obligations for each sector. This will also need to factor in any existing obligations for a given sector, noting the intent of Government is to "build on and do not duplicate existing regulatory frameworks" according to the Consultation Paper.

Providing proper comments about regulatory cost impact will also require further detail on developed options before this can be properly answered. As one member commented, it is impossible to estimate costs of such measures without the detail. This comment would equally apply to the other reforms proposed in the Consultation Paper.

We would also propose that any compliance costs created by new regulatory obligations should be fully funded/compensated by the regulator as it is done for national interest and security reasons and creates a regulatory burden on business. This will ensure that Government properly implements in practice its deregulation/red tape reduction policy agenda.

Therefore, at this stage, we consider that further work is required to be undertaken by Government on Initiative 1.

5. Initiative 2: Enhanced cyber security obligations – Situational awareness and Participation in preparatory activities (Consultation Paper Questions 22-28)

In addition to the PSO, the Consultation Paper seeks views on other measures to help protect Australia's most critical entities prepare for cyber attacks. The Paper provides examples where situational awareness can be improved through information sharing initiatives. Preparatory activities may include participating in cyber security activities with Government and co-developing a playbook of response plans.

Overall, we support partnering with Government on the above collaboration initiatives. However, in any form of collaboration, it is important that there are safeguards and assurance for organisations engaged in this activity to encourage participation. Such safeguards and assurances may include:

- safe harbour against being penalised as a result of sharing live threat information;
- the technical methods of threat sharing should not introduce new security issues;
- contextual information around threat sharing is provided and in return the information should be actionable and timely; and
- improved transparency on how live data can be shared and used to assist affected entities.

6. Initiative 3: Cyber assistance for entities – Establish the capability to disrupt and respond to threats (Consultation Paper Questions 29-36)

Initiative 3 features two elements: entity action and government action. Where there is an imminent cyber threat or incident, the Consultation Paper proposes for Government to direct entities to ensure action is taken to minimise its impact, and entities may also request Government to make that direction too – these entities would be given immunity in undertaking such actions and these actions would have to be within the entity's reasonable capability. In more limited circumstances, where Government identifies an immediate and serious cyber threat, Government may declare an emergency and take direct action to protect a critical infrastructure entity or system in the national interest (subject to robust checks and balances).

The Consultation Paper raises a number of questions relating to these two elements, including the circumstances by which direct actions will arise, the nature of such actions, regulatory oversight and safeguards, and risks to industry arising from these actions.

The proposed approach under Initiative 3 raises several concerns that require further clarification and development. These include:

- For a direction to take action, there is an assumption that an organisation has the required capability (i.e. technology, processes and people) to undertake that direction. Such capability needs to be included as the baseline for all entities.
- The description in the Consultation Paper is very broad and it is unclear the extent that the Government will be empowered including responsibilities of a company's personnel and the Government's own capability (including personnel) to properly operate in a safety critical environment. Questions also arise as to the level of accountability of Government should there be unintended consequences arising from the Government's actions if things go wrong.
- If Government plans to indemnify Ministers and public servants with respect to government assistance, this infers that there is a recognition that risk of errors could arise and Government may be seeking to limit its own risks of liability. However, this leaves businesses exposed without equitable remedy; businesses will therefore need to disclose that risk to their shareholders and stakeholders, potentially suffering consequences such as increased cost of capital as shareholders perceive such risk. This will need to be included as part of any cost-benefit assessment.
- There is an assumption that the Government has the capability (i.e. personnel, skills and experience) to operate critical infrastructure.
- It is unclear how a serious or critical incident would be classified. For instance, would a ransomware attack be considered as such an incident? More detail is required on defining these circumstances and at what point action would be taken by government.
- Collaboration in this area between critical infrastructure organisations and the government will be critical to successful implementation of Initiative 3. This Consultation Paper intends to improve collaboration, but it is unclear how this will be achieved.

Finally, should Initiative 3 progress into legislation (including establishing a new power for a Minister, Government agency, Officer or other public servant for the purposes of national security), there should be proportionate oversight that offers robust and independent approval processes, and appropriate safeguards and constraints. These include:

- The Intelligence National Security Legislation Monitor (INLSM) and the Parliamentary Joint Committee on Intelligence and Security (PJCIS) should be empowered to review the effectiveness and proportionality of proposed legislation and, as required, subsequent reviews of legislation that may be passed through Parliament.

- Proper independent oversight (e.g. judicial review) should be included in any decision involving execution of powers by the Government agency, Officer or Minister. The assigned judge would create a "double lock" and its decision would be binding i.e. the decision ought to be preceded by Ministerial execution of a power.

- Other safeguards and constraints to be developed in consultation with industry such as limits on powers, scope of government actions, clearly specified circumstances (including with a high threshold) that would trigger such government actions, and time-limited duration of powers.

If you would like clarification about this submission, please do not hesitate to contact me or our Lead Adviser – Industry Development and Defence Industry Policy, Charles Hoang ([redacted], [redacted]).

Yours sincerely,

[redacted]

Louise McGrath
Head of Industry Development and Policy