For reply please quote*: SP/BS – TF/20/18767 – DOC/20/183967*

Queensland Government

Department of the
Premier and Cabinet

Mr Michael Pezzullo AO
Secretary
Department of Home Affairs
michael.pezzullo@homeaffairs.gov.au

Dear Mr Pezzullo

Thank you for your email of 12 August 2020 advising me of the release of the Consultation Paper - *Protecting Critical Infrastructure and Systems of National Significance*.

I note that the Federal Government intends to shortly introduce legislation to amend the *Security of Critical Infrastructure Act 2018* (Cth) to impose an all hazards positive security obligation and a number of cyber security responsibilities on the owners and operators of critical infrastructure.

I am concerned that the compressed Federal Government timeframes in relation to this matter has limited opportunities for broader in-depth consultation including with the industries most directly affected. I am also concerned that there will be no opportunity for the states and territories to consider and comment on the draft bill, particularly when the Consultation Paper suggests that the jurisdictions may be asked to undertake some of the proposed regulatory and compliance responsibilities on behalf of the Federal Government.

Given the current fiscal environment, concerns have also been raised with the possible cost implications for the owners and operators of critical infrastructure to address and mitigate risks that they might identify while discharging their positive security obligation. Ultimately these costs will in all likelihood be passed on to the consumer. Any mitigation strategies should be reasonable and proportionate.

Please find attached the consolidated response from Queensland Government agencies to the issues raised in the consultation paper (**Attachment A**).

Once again, thank you for bringing this matter to my attention and I welcome the opportunity for further collaboration on this important initiative.

Yours sincerely

[redacted]

Dave Stewart
Director-General

***Encl**

1 William Street Brisbane
PO Box 15185 City East
Queensland 4002 Australia
Telephone +61 7 3224 2111
Facsimile +61 7 3229 2990
Website www.premiers.qld.gov.au
ABN 65 959 415 158

ATTACHMENT A

Queensland Government agency level response to the Consultation Paper: Protecting Critical Infrastructure and Systems of National Significance

---

This submission is a consolidated Queensland Government agency response to the Consultation Paper – *Protecting Critical Infrastructure and Systems of National Significance* prepared by the Department of the Premier and Cabinet. It does not propose a binding Queensland position in relation to the proposed reforms, but instead poses a number of issues that require further consideration by both the Australian Government and the Queensland Government.

All references to 'Government' both in the context of the Consultation Paper and in response to the questions below are taken to be references to the Australian Government unless otherwise specifically stated.

General Comments

Queensland Government agencies are already generally aligned with the principles outlined in the Consultation Paper through requirements under the *Financial Accountability Act 2009* (Qld) and compliance with the Queensland Government's Information Management Standards.

While noting the Australian Government's intention to impose a positive security obligation on the owners and operators of critical infrastructure, it is unclear from the Consultation Paper which critical infrastructure assets will be captured by the proposed amendments to the *Security of Critical Infrastructure Act 2018* (Cth). Additional advice regarding the scope of the legislation and the entities to be covered would be appreciated.

Consideration could also be given to the Australian Government taking a less prescriptive approach to the setting of the proposed standards to give effect to the positive security obligation and associated principles. Rather than regulating for a set of prescriptive standards in subordinate legislation, guidelines could be developed to assist the owners and operators of critical infrastructure to meet their positive security obligation. This approach has the advantage of providing greater flexibility, while reducing the level of regulatory burden.

Queensland Government agencies would welcome further consultation on the proposal that states and territories take on regulatory responsibilities on behalf of the Australian Government in relation to certain critical infrastructure entities. If regulatory responsibilities for these matters were to be undertaken by any Queensland Government regulator on behalf of the Australian Government, Queensland would expect the regulator to be fully resourced by the Commonwealth to undertake these tasks.

Given the current fiscal environment, there are also concerns with the possible cost implications for the owners and operators of critical infrastructure, both in meeting the additional regulatory burden, and costs associated with addressing and mitigating any risks that they might identify while discharging their positive security obligation. Any cost will ultimately be passed on to the end user.

Any mitigation strategies should be reasonable and proportionate given the risks associated with the identified hazard occurring, noting it is proposed to take an all-hazards approach rather than limiting the focus to security-related risks. While this may be relatively straight-forward when considering security risks associated with possible foreign interference and espionage, it may be far more complex and costly when considering the range of natural hazards faced by some critical infrastructure providers, particularly those providing services in the more natural disaster prone parts of the country.

Queensland Government agency level response to the Consultation Paper: Protecting Critical Infrastructure and Systems of National Significance

Queensland has concerns that the inclusion of natural disasters within the scope of the regime, via the proposed all-hazards approach, may unnecessarily complicate the proposed framework. While the application of the three framework elements (positive security obligation, enhanced cyber security obligations, and government assistance following a cyber-attack) are clearly applicable to cyber and human-induced threats, their application to natural disaster resilience is unclear. The Consultation Paper fails to indicate how a positive security obligation would apply, in practice, to natural hazard resilience.

Queensland Government agencies support the Australian Government using its resources and cyber capabilities to assist significant cyber situations to be resolved in the national interest. Unfortunately, insufficient detail has been provided in the Consultation Paper about how the proposed powers will operate to enable further meaningful comments.

Responses to the 36 Questions posed by the Consultation Paper

Who will the enhanced framework apply to?

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)?*

    - The risk to critical infrastructure from natural hazards is well understood, however, there is limited evidence either presented in the consultation paper or publicly available to support the security and sovereignty considerations that necessitate the inclusion of all of the proposed industry sectors in a new regulatory regime.

    - The definition would also benefit from a common understanding about what is considered vital to Australia's economy, security and sovereignty to enable a common understanding to be reached when considering relevant sectors.

    - In Queensland, critical infrastructure policy consideration also includes sectors such as mining and essential manufacturing (coal and key mineral mining, liquid fuels, heavy industry, industrial and AGVET chemicals), and essential government services such as emergency services.

    - Any decision to deem additional sectors as critical (for example new and emerging manufacturing sectors) will require careful consideration of the costs and impacts on fragile sectors to compete globally.

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

    - While the current definition of critical infrastructure contained in the Australian Government's *Critical Infrastructure Resilience Strategy* is suitable for a strategy document, the definition may need to be further refined as part of the proposed regulatory approach.

    - The current definition is subjective and relies on a number of interpretations and assumptions, generally made from the perspective of Australian Government agencies when considering if an asset is critical or not. This definition has led to differences in interpretation about what assets constitute critical infrastructure.

    - The current definition also requires owners and operators to have knowledge about how the loss of their infrastructure may impact on Australia's ability to conduct national defence and

ensure national security or be able to assess what impact the loss will have on the 'wellbeing of the nation".

- The proposed legislative approach requires a definition that provides legal certainty about what is and is not captured by the term critical infrastructure. The legislative approach may also benefit from the inclusion of assessment criteria to aid in determining if a critical infrastructure asset is within the scope of the legislation, for example:
  - proportion of population directly affected by the total loss of the asset / service, e.g. over 10% of the population affected is considered a 'high' impact;
  - likely duration of outage – the estimated time to replace the critical service / supply of product provided by work around or delivered by alternate infrastructure;
  - economic consequence of the loss of the asset, as a proportion of Gross Domestic Product (GDP) - based on the assumption of the total loss of the asset / service; and
  - inter-dependency influence – a representation of the anticipated impact of the loss or degradation of the service to other critical services or sectors. For example, energy and water have an 'extreme' inter-dependency influence because every other sector relies directly on this critical infrastructure.

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?*

- Queensland Government agencies support the proposal to map the interdependencies and the possible impact that a compromise of one entity / critical infrastructure asset may have on another. This will take some time and it is unclear if the current round of workshops with entities and peak bodies has been sufficient to properly map these relationships.

- Other factors that may need to be considered would include redundancy. The consequence of loss (combining population affected; likely duration of outage; economic loss etc.); inter-dependency and level of redundancy are generally considered in criticality assessment methodology.

- Redundancy of supply is particularly important because although a service may appear essential, if it can be supplied from several different critical infrastructure sources, the loss of one critical infrastructure source of supply may not result in a significant impact. Conversely, scarcity of alternative resources in the vicinity may increase the criticality of an asset.

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

- Queensland currently utilises a multifaceted, decentralised approach to the protection of critical infrastructure, with an emphasis given to critical infrastructure resilience from natural hazards or security risks including digital and supply chain disruption.

- The *Disaster Management Act 2003 (Qld),* and associated policies and guidelines, provide the basis for state-wide all-hazards risk assessments to be carried out, preferably using the Queensland Emergency Risk Management Framework to identify hazards and vulnerabilities at the local level, including those faced by critical infrastructure.

- The Queensland Strategy for Disaster Resilience and associated implementation plan, Resilient Queensland 2018-2021, seeks to enhance Queensland's resilience to natural hazards, including the resilience of critical infrastructure.

- Queensland also operates a number of regulatory regimes that contribute to ensuring critical infrastructure associated with water, electricity, gas, ports and transport infrastructure are reliable and sustainable.

- Key road and rail mass passenger transport services are currently declared as security identified surface transport operations (SISTOs) under the *Transport Security (Counter Terrorism) Act 2008* (Qld) and as such, already have physical and personnel security arrangements in place.

- The Queensland Police Service (QPS) also engages with the owners and operators of critical infrastructure and crowded places across the state, primarily through its Security and Counter-Terrorism Network. The QPS provides advice about security threats, and assists owners and operators to assess their risks and undertake any necessary mitigation activities.

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

- Deciding issues of criticality will depend on the nature of the risks being considered and the perspective from which it is considered. Critical infrastructure assets will have differing risk profiles depending on the hazard being faced. Significantly more work and consultation will be required to consider and assign attributes of criticality including development of detailed risk matrices.

- Criticality could be considered in the following context:
  - value to the system
  - system impact (for example, if affected, what would be the impact and how far reaching would the consequences be, that is, what would be the impact on the relevant sectors, governments and the community)
  - what is the capability redundancy? Does it exist? If not, what would be the outcome if the critical infrastructure is lost forever, or if it is so cost-prohibitive we cannot replace it? What would be the impact of the recovery time?

- An additional consideration could include an assessment of critical 'enablers' that support the functioning of existing critical infrastructure and helps to safeguard our future economic and social wellbeing. The criticality assessment of an enabler will require a different approach to existing critical infrastructure, but should be based on the contribution to essential goods and services.

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

- Queensland Government agencies would welcome the opportunity to further discuss this issue with the Department of Home Affairs and other relevant Australian Government agencies.

Queensland Government agency level response to the Consultation Paper: Protecting Critical Infrastructure and Systems of National Significance

Government-Critical Infrastructure collaboration to support uplift

7. *How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?*

- A revised Critical Infrastructure Resilience Strategy could be used to guide the implementation of the proposed new framework. This could include the development and provision of tools and guidelines separate from the regulator to assist entities to measure, characterise, manage and mature their critical infrastructure management systems.

- If the TISN was to play a more active role in the coordination and communication of vital research and provide a standardised approach to information sharing across critical infrastructure sectors, it would improve operational effectiveness and assist in alleviating some of the barriers to information sharing.

- The TISN could also act as a subject matter expert for Government and could be used to facilitate the development of a cross-sector strategy focusing on inter-dependencies.

8. *What might this new TISN model look like, and what entities should be included?*

- A new model for industry and government engagement around the protection of critical infrastructure may need to be developed to replace the current TISN structure which is based on voluntary engagement, rather than statutory obligation as proposed.

- This new model should reflect the additional industry sectors and provide clearly defined and agreed roles, including the role of state, territory and local governments.

- An expanded and enlivened TISN needs to be responsible to an appropriate national body under the auspices of the National Federation Reform Council to ensure it has 'national' rather than just Australian Government oversight, and it equally reflects the important roles of all levels of government (including the Australian Local Government Association) and business.

- A wide range of small to medium enterprises (SMEs) operate in the different critical infrastructure industry sectors, but they are unlikely to be directly affected by this legislation. To ensure the flow-on of relevant information and broader engagement with SMEs, the relevant industry sector associations and peak bodies should be engaged as an extension of the TISN.

- The TISN Secretariat should be provided by the Department of Home Affairs rather than by separate industry sectors to enhance consistency and coordination across the TISN sectors.

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?*

- More information, research and collaboration will be required to fully understand and manage risks associated with cross-sector dependencies. The current TISN structure, based on industry sectors, does not readily lend itself to consider cross-sectorial issues.

- This work should build off the previous work of the Critical Infrastructure Program for Modelling and Analysis (CIPMA) to map inter-dependencies and identify common nodes and network

linkages, the disruption of which could cause cascading failures across multiple CI and sectors. CIPMA should be reinvigorated and the resulting models used to guide infrastructure planning and preparation for events with wide-spread impacts.

- While natural hazard risks are broadly understood, more specific security information may be needed to enable industry to fully understand and appreciate man-made security risks and where cross-sector dependencies may exist.

- All levels of government could also identify and promote opportunities for private sector investment and partnerships in regard to critical infrastructure and assist in streamlining policy and procurement conditions to reduce red tape and facilitate greater collaboration.

- All governments could also assist with the development of disaster risk reduction tactics. Other specific activities could include:

  - conducting joint exercises
  - ensuring the focus of audits against standards is supportive and promotes continual improvement
  - hosting regular Community of Practice forums that provide strategically focused guidance and threat environment updates
  - sharing hazard analyses across infrastructure sectors.

Positive Security Obligation

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

- Queensland Government agencies note the four broad principles referred to in the Consultation Paper, however, would like the opportunity to consider and comment on how the proposed principles are ultimately drafted in the proposed Bill to ensure that there are no unintended adverse consequences.

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

- This is difficult to comment on without more specific information about what will ultimately be contained in the Bill and subsequent supporting subordinate legislation. Significantly more detail would be required to enable proper regulatory impact assessments to occur.

- Consideration must also be given to how a risk is to be managed if it is outside the organisation's control. This situation is more likely to arise when consideration is being given to supply chain risks.

- Many of the current requirements rely on collaboration and cooperation between state and territory governments and industry sectors. The proposed regulatory regime may change the nature and balance of that cooperative relationship.

- Whilst simplicity, transparency, accuracy and stability are reasonable criteria, consideration should also be given to:
  - the cost of compliance;

- adequacy of current risk mitigation practices; and
- whether the additional regulatory response is appropriate given the potential impact on the community and economy.

- The Consultation Paper does not clearly indicate what critical infrastructure owners, operators or regulators should expect, in practical terms, of a positive security obligation to protect against natural hazards.

12. *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?*

- Industry sectors are at differing levels of maturity with respect to their considerations of the broad range of risks to be covered by the positive security obligation and associated principles.

- In Queensland, Government Owned Corporations (GOCs) own and operate the majority critical infrastructure relating to energy and water supply, and their approach to risk management generally reflects these principles.

- In the cyber space, a number of organisations are adopting ISO27001-2018 for cyber security systems.

- Many organisations apply these principles in relation to those risks they assess will cause the greatest loss or commercial gain to their organisation, rather than necessarily the most significant impact that loss may have on society or the national economy.

- Many organisations have implemented standards-based controls like ISO27001.

13. *What costs would organisations take on to meet these new obligations?*

- Given the current fiscal environment, Queensland Government agencies have raised concerns with the possible cost implications for the owners and operators of critical infrastructure both in meeting the additional regulatory burden, and costs associated with addressing and mitigating risks identified while discharging their positive security obligation.

- There are also concerns that any cost may ultimately be passed on to the end user.

- Queensland would welcome the feedback from sector organisations regarding the specific costs of compliance they envisage.

14. *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?*

- Queensland Government agencies are already generally aligned with the principles outlined in the Consultation Paper in support of the positive security obligation through requirements under the *Financial Accountability Act 2009* which contains risk and business continuity management obligations and compliance with Queensland Government Information Management Standards.

- The small number of non-government sectors that are security regulated tend to incorporate standardised, compliance-based approaches (e.g. air passenger screening), rather than following a principles-based outcomes approach.

- Defence-aligned industries in Queensland are already required to meet security obligations in line with these principles.

Regulation

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

    - The extent that the proposed regulatory model will reduce duplication is unclear. Multiple regulators across Commonwealth, state and local government entities could lead to inconsistency and fragmentation and make assessment of cross-sectoral interdependencies more difficult.

    - Consideration could be given to a less prescriptive approach to the setting of the proposed standards. Rather than regulating for a set of prescriptive standards in subordinate legislation, guidelines could be developed to assist the owners and operators of critical infrastructure to meet their positive security obligation.

    - This approach has the advantage of providing greater flexibility and reduce the level of regulatory burden.

    - In the energy sector, consideration should be given to whether the existing market regulators could manage these issues to avoid duplication.

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?*

    - Queensland Government agencies have concerns that adding the roles of security education, guidance, monitoring and enforcement to a regulator, who will still be required to undertake their previous roles regarding safety, could result in increased economic and operational impacts on both the regulator and the critical infrastructure entity.

    - More consideration needs to be given to the proposed regulatory model suggested in the Consultation Paper. The proposed approach may also require state and territory governments to review their regulatory frameworks to give effect to this proposal. This review will be a time consuming, costly and burdensome process.

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?*

    - The need for a full regulatory and compliance approach proposed across all critical infrastructure sectors and across all hazards has not been fully demonstrated by the Consultation Paper.

- Without more specific detail as to the proposed role, powers and functions of the regulatory bodies, Queensland Government agencies are generally not in a position to suggest the most appropriate regulator across the proposed sectors.

- However, in the energy sector, the Australian Energy Market Operator and the Australian Energy Regulator may be a suitable regulator.

- Another alternative is to express the expected standards/obligations in terms of ISO (or equivalent) standards. By doing so, each business will know what actions it must take to ensure the minimum level of preparedness or capability is achieved and avoid the complexity and cost of a formalised regulatory compliance model.

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

    - If regulatory responsibilities for these matters were to be undertaken by any Queensland Government regulator on behalf of the Australian Government, Queensland would expect the regulator to be fully resourced by the Commonwealth to undertake these tasks.

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

    - The Australian Government needs to provide a platform for standardised risk assessment to help ensure the use of a consistent methodology to enable outcomes of risk assessments to be comparable across entities and sectors.

20. *In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?*

    - Investment by entities in the development of a security culture may be a more important mitigation factor which should be encouraged.

    - While a useful starting point, national security and criminal history assessments are a point in time assessments which may only add limited value. The first Australian ever convicted of a terrorism offence (in Lebanon) held an Australian Aviation Security Identification Card.

    - Any additional requirements on businesses for security checks would need to be adequately supported (resourced) by vetting agencies to minimise disruption to business due to lengthy delays in processing applications.

21. *Do you have any other comments you would like to make regarding the PSO?*

    - The Positive Security Obligation needs to be supported by an information and education strategy to improve capability of organisations to meet this new requirement.

    - A staged approach would also enable all sectors to adhere to compliance requirements, providing an opportunity for those organisations who are not as mature in this area to develop their compliance approach.

Queensland Government agency level response to the Consultation Paper: Protecting Critical Infrastructure and Systems of National Significance

Enhanced Cyber Security Obligations

22. *Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?*

- A broader awareness and information sharing program (outside of the existing TISN) to ensure that all organisations are aware of the enhanced cyber obligations and systems are put in place to ensure engagement with those entities that may not otherwise engage through the voluntary TISN.

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

- Critical infrastructure entities will require a broad range of timely threat intelligence information from relevant Australian Government agencies including information about threats, tactics and techniques being used by nefarious actors.

24. *What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?*

- Queensland Government agencies would welcome the views of the owners and operators of critical infrastructure in relation to this matter.

- Consideration could be given to sharing agency specific trend data that relates to the current threat environment (where appropriate). However, procedures and agreements will need to be put in place regarding how the data would be used and shared including technical considerations.

25. *What methods should be involved to identify vulnerabilities at the perimeter of critical networks?*

- Improved cross-sector collaboration at the stage of risk assessment would lead to improved identification of system vulnerabilities, interdependencies and mutually beneficial risk management strategies.

- A risk-based approach using ASIO T4 measures and the applications of security zones would also be beneficial.

26. *What are the barriers to owners and operators acting on information alerts from Government?*

- This is not a matter that Queensland Government agencies can comment on in detail without further consultation and engagement with the owners and operators of critical infrastructure.

- Owners and operators may be reluctant to engage if acting on information alerts where they are seen as yet another cost imposed on the business without a tangible benefit, and there may be conflicting expectations/standards between the governments' and private sector's risk appetite.

- Inconsistent messaging across agencies can also be a barrier to implementation.

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

- Co-design requires a high degree of transparency. This may be restrictive due to consumer sensitivities, intellectual property concerns and commercial/market strategies between competitors.
- The playbooks should include and reflect state and territory Government roles and arrangements including disaster management arrangements in response to a significant cyber incident.
- Clarity would be required regarding how critical infrastructure owners/operators tie into national and state arrangements across prevention, preparedness, response and recovery activities. This is an ongoing gap and leaves the sector in a reactive mode.
- On a more practical level, specific playbooks focusing on a Supervisory Control and Data Acquisition (SCADA) attack, including unplanned & untriggered reboot of SCADA servers, multiple SCADA alarms indicating critical failures and failure of automated processes in SCADA including the handing of control back to water operators through the Human Machine Interface would be useful.

28. *What safeguards or assurances would you expect to see for information provided to Government?*

- Queensland Government agencies expect that any information provided to relevant Australian Government agencies in compliance with these provisions will be treated with appropriate levels of confidentiality, be securely held and that entities be consulted prior to any public release of that information.
- Consideration may also need to be given to providing statutory protections to the operators of critical infrastructure around any information that they are required to disclose.

Cyber Assistance for entities

29. *In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?*

- Queensland Government agencies support the Australian Government using its resources and cyber capabilities to assist significant cyber situations to be resolved in the national interest.
- Unfortunately, insufficient detail has been provided in the Consultation Paper about how the proposed powers will operate to enable further meaningful comments.
- Details in relation to the operation of these powers should be contained in the *Security of Critical Infrastructure Act 2018* (Cth) rather than in subordinate legislation and consultation should occur with the states and territories prior to these provisions being enacted.

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

- Consideration should be given to appointing an appropriate elected official (Minister responsible designated in legislation) acting on expert advice from the Australian Cyber Security Centre and other relevant agencies including agencies involved in consequence management.
- A cyber-attack that significantly impacts our economy, security or sovereignty could have major consequences for the community and require States, Territories and Local Governments to activate emergency, and possibly disaster, response arrangements.
- The coordination of Australian Government and critical infrastructure entity actions with States, Territories and Local Governments response and recovery activities are essential to minimise the adverse consequences of a significant cyber-attack.
- Further planning and preparation by all levels of governments and critical infrastructure entities should occur, possibly coordinated through the National Cyber Security Committee to ensure high levels of coordination in response to a significant cyber threat or attack.

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

- Oversight arrangements would need to be considered once the detailed regulatory regime is settled. However, there are a number of options to be considered, including ensuring the responsible Minister provides a report annually to Parliament and a possible role for the Inspector-General of Intelligence and Security to oversee and report on the use of these powers.

32. *If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber-attack, do you think there should be different actions for attackers depending on their location?*

- If a perpetrator is located in Australia, the need to respond in coordination with State and/or Territory police will be required. The disruption activity should have regard to policing objectives to gather evidence of an offence.
- Counter-measures should be proportionate to the threat and tailored to mitigate the ongoing threat of the perpetrator.

33. *What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?*

- Consideration could be given to offering legal protections from civil litigation for any reasonable mitigation activities that may need to be taken in the envisaged extreme situations where these powers might be used.

34. *What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?*

- See the answer to Question 31

35. *What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?*

- Government imposed mitigation strategies can impact on international competitiveness through additional costs. The proposals also raise sovereign risks to potential investment in Australia because of the inherent requirement for the companies to act in Australia's sovereign interest under the proposed changes.

- Open access to research and development from foreign industry/government can compromise potential competitive intellectual property or infrastructure security.

36. *Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?*

- Implementation of this proposed model should consider correlation with existing roles and responsibilities; industry approaches; and approaches to the management of risk.

- Owners and operators of critical infrastructure may need to consider the potential unintended consequences of government decision-making to their sector during times of national interest emergencies. These considerations will initially need to be given during the planning phases for any potential response.