Annie Chi
Manager, Information Systems (IS)

September 14, 2020

Richard Feakes
First Assistant Secretary
Aviation and Maritime Security Division
Department of Home Affairs

Via e-mail ci.reforms@homeaffairs.gov.au

Dear Mr Feakes,

Response to Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

Chevron Australia (Chevron) welcomes the opportunity to provide the following responses to the matters raised in the Response to Protecting Critical Infrastructure and Systems of National Significance Consultation Paper.

Chevron is one of the world's leading integrated energy companies and has been present in Australia for more than 60 years. Chevron Australia operates the Gorgon and Wheatstone LNG and domestic gas projects; manages its equal one-sixth interest in the North West Shelf Venture; operates Australia's largest onshore oilfield on Barrow Island; and is a significant investor in exploration.

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 discussion paper captures the functions appropriately and all relevant sectors have been addressed.

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

   It appears that the definition at page 11 focuses on the availability of what is classified as critical. Consideration must be provided to the confidentiality and integrity of the data associated with those critical assets where, if compromised, significant impact would still be suffered without the loss of the functionality of that asset e.g. confidentiality compromised in the banking sector or data transmission degraded in the communications sector.

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

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?*

   When identifying an entity, the 'consequence of compromise' needs to be a holistic assessment considering all reputational, legal, environmental, health & safety and national security impacts in addition to financial impacts.

   An entity's cyber-maturity level should also be considered when prioritising critical entities - those at a demonstrated higher level of maturity would be a lower priority.

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

   Chevron routinely tracks and prepares for threats of phishing, spearphishing, waterholing, business email compromises, ICS targeting, supply chain compromise, vulnerability exploitation, ransomware, password spraying and malware. Chevron tracks and prepares for nation state threat actors, hacktivists, cybercriminals, opportunist (lone hackers), and malicious and non-malicious insiders. Phishing and malware are the most common threats experienced by the business, with most incidents impacting only a small, isolated number of systems that are not mission-critical.

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

   Diversity of an entity's sector should be considered, in addition to the size of the entity or its supply contribution in isolation. For example, in a sector with multiple contributors, failure of an individual entity may not in itself lead to the negative impacts described in the paper.

   A standard assessment needs to be developed to ensure that all entities are assessed equally allowing for a fair comparison.

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

   Across the energy sector there are a number of gas producers and suppliers. However, there is less diversity in the owners of the pipeline used to reticulate the gas to industry and consumers. For example, Chevron's supply to the Dampier to Bunbury Pipeline (DBPL) is less critical than the pipeline infrastructure itself. Diversity of supply in criticality determination is a key consideration.

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

   An expanded TISN working in consultation with the ACSC would be of benefit to further the resilience of the Critical Infrastructure operators. We would welcome the opportunity to review the Critical Infrastructure Resilience Strategy.

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

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

Chevron would recommend working in consultation with the ACSC, with a sector-specific focus group similar to the OGSF.

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?*

   The Government should provide clear and regular information-sharing across sectors, while ensuring confidentiality of any information shared by entities.

   Government should share indicators of compromise and threat information with industry. Visibility to known or potential threats is the cornerstone of any cybersecurity program. Knowing that industry is generally responsible for protecting its infrastructure, being aware of latest threats is arguably the most important asset.

   Government should help entities by 'mapping' the dependencies between entities in order to identify key integration points (and any bottlenecks or weaknesses). The Government could orchestrate the mapping of these interdependencies at a national level, which would create a data-driven model of cross-sector risks and dependencies.

   Government should encourage the further expansion of industry-sharing opportunities like that provided by Australian Cyber Security Centre (ACSC). It could develop cost effective opportunities to upskill organisations to achieve baseline and more advanced skillsets to meet the threat environment.

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

    Yes.

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

    It is possible to make the proposed regulatory model work. The model is risk-based which is in line with Chevron's philosophy. It avoids a compliance approach which would tend to focus companies on implementing specific controls which may or may not actually address key threats.

    For the purposes of the paper, the requirements provide balance, however clear actionable direction will need to be provided in sector-specific guidelines, with the ability to recognise where an entity is at a mature state. For mature entities, it will not be beneficial to over-apply reporting and/or attestation requirements.

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?*

    For organisations in the energy sector that are operating at a high level of maturity, such as Chevron, the underlying processes and controls are already in place to meet these principles.

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

For smaller or less mature organisations there may be a significant time, cost and skill development demands.
For organisations of all levels, care should be taken to balance reporting requirements. More mature organisations could self-attest, whilst those of lower maturity may require assistance to implement the necessary processes and procedures.

All businesses within Australia will mutually benefit from an up-lift in cyber maturity. There are noted pockets of industries which are facing a relatively large expense to improve their cyber security posture.

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

Organisations such as Chevron which have implemented comprehensive security controls aligned with an industry standard framework should incur relatively little cost aligning with the new obligations.

Chevron would like to work with the Australian Government to implement a framework that will result in minimal expense in demonstrating competence.

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?*

Chevron adopted the NIST Cybersecurity Framework[1] (CSF) in 2014 as the foundation for its cybersecurity practice. The CSF is the anchor for Chevron's cybersecurity standards and controls. Architecture/strategy are presented in terms of the CSF's five functions of Identify, Protect, Detect, Respond, and Recover.

The CSF is outcome-based and consequently is in line with initiative 1 of the Consultation Paper. The CSF maps well to the principles-based outcomes listed in the Paper.

Consultation Paper Principle	Comparable NIST CSF Categories
Identify and understand risks	Risk Assessment (ID.RA), Supply Chain Risk Management (ID.SC), Asset Management (ID.AM),
Mitigate risks to prevent incidents	Protect Function (PR), Detect Function (DE), Respond Function (RS), Recovery Planning (RC.RP)
Minimise the impact of realised incidents	Backups are conducted and maintained (PR.IP-4); Response plans are in place, managed, and tested (PR.IP-9 & PR.IP-10); Coordination with stakeholders (RS.CO-4 & RC.CO-1)
Effective governance	Risk Management Strategy (ID.RM), Governance (ID.GV)

CSF includes additional categories/sub-categories addressing the Consultation Paper's Security Obligations of physical security (Physical access to resources is protected (PR.AC-

[1] https://www.nist.gov/cyberframework

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

2)), cyber security (Data Security (PR.DS), Software Development Lifecycle (PR.IP-2), Detect Function (DE)), Personnel Security (Awareness and Training (PR.AT), Cybersecurity included in HR practices (PR.IP-11), Cybersecurity roles are coordinated and aligned (ID.GV-2)), and supply chain security (Organization role in supply chain is understood (ID.BF-1), Supply Chain Risk Management (ID.SC)).

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

    It is possible to make the proposed regulatory model work. The model is risk-based which is in line with Chevron's philosophy and avoids a compliance approach which would tend to focus companies on implementing specific controls which may or may not address key threats. The key to making the approach work is giving companies the flexibility to choose how they meet the requirements. Companies should be allowed to use any framework which meets the Consultation Paper objectives whether this be NIST Cybersecurity Framework as in Chevron's case, ISO 27000, COBIT, Information Security Forum Standard of Best Practice, or any of the other cybersecurity frameworks. Companies should be able to demonstrate adequacy through maturity assessments conducted against their chosen framework.

    A worst case would be to require each company to follow a single framework or complete standardised forms. Company resources spent translating activities from one format to another do not improve and likely detract from security posture.

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?*

    Ensure that guidance leverages existing frameworks (NIST CSF, ISO 27001 et al). Guidance should not overburden entities which have already implemented such frameworks.

17. *Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?*

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

    Unless a specific regulator is in place and has cyber skills and expectations in place, the Government should look to the ACSC to provide this regulatory oversight.

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

    The Government can better support critical infrastructure through collation and sharing of relevant information in a timely manner and providing comprehensive play books on how best to deal with any developing situation, in addition to information on who, when and how to contact for relevant support. The focus should be on uplift of operators who do not demonstrate cyber maturity.

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

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?*

    Chevron would be interested in leveraging this information source.

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

    No.

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

    Government should share indicators of compromise and threat information with industry. Visibility to known or potential threats is the cornerstone of any cybersecurity program. Knowing that industry is generally responsible for protecting its infrastructure, being aware of latest threats is arguably the most important asset.

    Industry should continue to have the primary responsibility of responding to cyberattacks and protecting corporate assets. Government can assist by sharing information on latest threats and by maintaining response services which may be voluntary called upon by industry as necessary.

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

    Government should share indicators of compromise and threat information with industry. Visibility to known or potential threats is the cornerstone of any cybersecurity program. Knowing that industry is generally responsible for protecting its infrastructure, being aware of latest threats is arguably the most important asset.

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?*

    Chevron currently voluntarily shares crimeware and other threat intelligence with entities both only within the oil & gas industry and to other sectors. This does not include classified government information nor information from paid intelligence services but rather self-generated threat intelligence. Since Chevron already has a Threat Intelligence group, cost implications would be minimal only if an automated standard threat sharing platform were used (e.g., ThreatConnect or similar platform).

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

    Chevron employs several methods to identify vulnerabilities including penetration tests executed by external parties and internal vulnerability scanning. Care must be taken when searching for vulnerabilities on process control networks as these networks rely on real time

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

execution and scanning exercises can disrupt or take down such systems. Lab systems or digital twins should be used to scan for process control vulnerabilities, as this would allow identification of issues without jeopardising production systems.

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

    Organisational capability is the primary barrier. Larger companies like Chevron have their own internal security operations centre which are capable of assessing and acting upon government-provided alerts. Smaller companies may be unable to sustain their own security operations centre and consequently would not have the resources to act upon an alert.

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

    Chevron would like to work with the Australian Government to implement a framework that will result in minimal expense in demonstrating competence in line with suggestions contained within this document.

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

    There would need to be a non-disclosure arrangement together with liability protection from acting or not acting upon provided intelligence.

29. *In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?*
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?*
31. *Who should oversee the Government's 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?*
34. *What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these types of powers?*

    Addressing questions 29, 30, 31, 32, 34 collectively:

    Chevron has reservations about government unilaterally taking over response to a cyber incident. There is the risk of damage to process control systems (see answer to question 35) but there is also the possibility that the attack may not be restricted solely to Australia's critical infrastructure. Chevron provides energy services across the world and it is conceivable that the adversary may be launching a global attack. Response to such a global attack would need to be coordinated across company systems, therefore a policy that allowed government to unilaterally take over response in Australia would preclude a coordinated response across the company and may lengthen actual recovery of services. As an example, the Australian Government response may eradicate the intruder on Chevron Australia's systems, but the attacker may still persist within other Chevron systems in other countries and could relaunch

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

the attack into Australia. It is unclear whether the Australian government would be able to address Chevron systems in other countries.

The concept of a government declaring an emergency and taking over response is unusual. US Critical Infrastructure regulation, as an example, does not have such a concept. Critical infrastructure companies are required to protect their own environments. Government resources are available to assist but only on a voluntary basis.The Government may take over incident response at a company but only if the Government were asked to work the incident by the company.

Coordinated response in the US is usually handled through Information Sharing and Analysis Centres (ISAC). Each sector has such a body which generally provides an ability for industry members to share threat and other intelligence information among themselves and with the government. ISACs tend to have their own security operations centres and can coordinate response if several members report similar threats/attacks. An example of the latter is the role the Financial Services ISAC took to help address Distributed Denial of Service attacks against US financial institutions in 2012/2013.[2]

Chevron's view is that private industry should continue to have the primary responsibility of responding to cyberattacks and protecting corporate assets. Government can assist with sharing information on latest threats so that corporations may be better prepared as well as maintaining response services which may be voluntary called upon by a corporation if necessary.

Government should have the primary responsibility for deterring cyber attacks contemplated by nation states and organized criminal elements. Government has multiple cyber and non-cyber means (diplomatic, economic, military and law enforcement), many of which are not available or not advised to be used by private firms, to dissuade entities from particular actions or to punish after such events.

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

Liability protection from acting or not acting upon provided intelligence.

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?*

The Government will not necessarily understand the operations and issues within process control systems and may damage systems in their response. The Government might be able to deflect the assailant but would possibly cause the same damage/disruption that the attacker attempted via a heavy-handed response.

[2] https://www.alston.com/-/media/files/insights/publications/2013/06/evolving-ddos-attacks-provide-the-driver-for-finan/files/evolving-ddos-attacks-provide-the-driver-for-finan/fileattachment/evolving-ddos-attacks-provide-the-driver-for-finan.pdf

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]

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?*

    Private industry should continue to have the primary responsibility of responding to cyber attacks and protecting corporate assets. Government can assist with sharing information on latest threats so that corporations may be better prepared as well as maintaining response services which may be voluntary called upon by a corporation if necessary.

    Government should have the primary responsibility for deterring cyberattacks contemplated by nation states and organized criminal elements. Government has multiple cyber and non-cyber means (diplomatic, economic, military and law enforcement), many of which are not available or not advised to be used by private firms, to dissuade entities from particular actions or to punish after such events.

Thank you for the opportunity to provide Chevron's views on these important issues.

Sincerely,

cc:

Annie Chi
Manager, Information Systems
Australia Business Unit
250 St George's Terrace, Perth, WA 6000
Tel [redacted]