Our Reference: SC-DHA-0001

17 September 2020

Hamish Hansford
First Assistant Secretary
National Resilience and Cyber Security Group
Department of Home Affairs
PO Box 6021
Parliament House
Canberra ACT
2600

Dear Hamish,

Sapien Cyber Response - Consultation Paper - Protecting Critical Infrastructure and Systems of National Significance

Please find attached Sapien Cyber's Response to the Department of Home Affairs Consultation Paper "Protecting Critical Infrastructure and Systems of National Significance".

Sapien Cyber is founded upon Edith Cowan University's (ECU) 20 years of world-leading research in cyber security and is ECU's commercialisation vehicle for that research. Sapien is a commercial entity, bringing together a team of industry experienced practitioners to develop a unique, sophisticated world-leading solution for Operational Technology (OT), Information Technology (IT) and Building Management Systems (BMS) environments.

Our technology platform provides unparalleled visibility, threat detection and response capabilities, reducing our clients' risks through a sophisticated layered approach to cyber security.

We welcome the opportunity to participate and contribute to the Consultation Paper, with the intent of protecting the essential services that all Australians rely upon by uplifting the security and resilience of critical infrastructure.

Sapien Cyber believes there are important aspects defining the protection of our nation's critical infrastructure that are directly aligned to the terms of reference, with respect to national resilience, assuring supply chain integrity and protecting our national infrastructure and services from cyber threats.

SAPIEN CYBER ACN 615 836 827
ECU
Joondalup WA
Australia 6027
1800 378 200
info@sapiencyber.com.au
sapiencyber.com.au

SAPIEN

Sapien's focus is on the building of a domestic sovereign Australian cyber security industry which is essential for the protection of Australia's national interests. This particularly applies to vital or critical infrastructure. With the threats to such infrastructure from both state and non state actors only on the increase, cooperation between the Commonwealth and Australian industry on cyber security protection of critical infrastructure is essential to protect our national security and economic interests.

Yours sincerely,

[redacted]

Glenn Murray
CEO/MD
SAPIEN CYBER

SAPIEN

Department of Home Affairs

Protecting Critical Infrastructure and Systems of National Significance

Consultation Paper Response

Doc No. CS-DHA-0001 v1.0
16-September-2020

Document Management and Control

Version	Issue Date	Description
1.0	14-Sep-2020	Initial
2.0	16-Sep-2020	Final

Contents

1. Introduction

Sapien Cyber ("Sapien") welcomes the opportunity to respond to the Department of Home Affairs Consultation Paper "Protecting Critical Infrastructure and systems of national significance", which directly aligned with our company's priority focus.

Sapien is an internationally recognised industry leader providing cyber security solutions for protecting Operational Technology (OT), Building Management System (BMS) and Information Technology Infrastructure (IT).

Our mission is to "protect the world we live in" by evolving faster than the speed of threat. Our critical services provide systematic awareness of relevant and reliable information to understand a cyber security event in real-time, with context specific to each of our client's operational priorities. This is supported by an in-depth understanding of the critical decision chain that underpins our innovation and technological developments in areas such as large-scale software-driven systems, secure communications and sectors, including but not limited to Industrial Control Systems (ICS), Industrial Internet of Things (IIoT) and Supervisory Control and Data Acquisition (SCADA).

Sapien's next generation technology platform adopts a truly unique 'system of systems' architecture, fusing passive network monitoring technology with a multi-intrusion detection sensor capability, machine & deep learning, malware analysis, deep packet inspection and human intelligence. This provides our clients with unparalleled network awareness and threat visualisation and contextualisation. Innovatively surpassing other market solutions, Sapiens' solution monitors Open System Interconnection (OSI) level 2 network traffic to identify indicators of compromise. Sapien utilises deep packet inspection techniques with nanosecond precision after passively ingesting network traffic and processing multiple streams of the traffic in parallel. This method assures that the system has no impact on running assets as there are no active queries that could degrade operations.

2. Who will the enhanced framework apply to?

2.1 Response by Sapien

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 sectors cover the bulk of critical infrastructure domains.

   However, Sapien has identified a number of interdependencies or even direct dependencies between services operated at the front of a business and those on which it in turn relies. Critical and important systems are increasingly virtual in nature, such that these services are elevated to a critical supply status and also represent critical information in their own right. These systems also tend to be meaningless without the information they carry. This is a trend that will continue.

   Sapien regularly engages with clients who manage critical infrastructure to protect and secure systems integral to their ongoing safe operations. This provides Sapien with a detailed view of system and service dependencies within information and virtual supply chains.

   The Consultation Paper has identified a superset of the assets currently covered under the Act (e.g. critical electricity assets, critical gas assets, critical ports, critical water assets, assets

declared under Clause 51 to be critical infrastructure assets and assets prescribed by the rules of the Act) to all the sectors noted on page 11 of the Consultation Paper.

Sapien defines critical infrastructure as the services and systems on which Australia relies for our nation's security, wellbeing, and economic resilience. In this regard, the increased list of 11 sectors provides appropriate coverage, although manufacturing is indeed critical where it is part of a supply chain for goods.

However, this may not encompass the whole manufacturing sector. Similarly, there will be supply chains behind some of the other sectors that may be critical, for example does food and grocery only relate to retail services or does it also encompass aspects of transport and agricultural sectors? And does transport also include shipping, which is 98% foreign owned/controlled? This line of questioning suggests that although there will be certain services that are critical, government will need to take care in defining these sectors in order to avoid diluting the importance of truly critical services.

As an example, the US definition for critical infrastructure includes systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

In relation to the definition of critical infrastructure, the US Department of Homeland Security (US DHS) describes critical infrastructure as "the physical and cyber systems and assets vital to the US".

While the above is inferred in the definition of Australian critical infrastructure, the definition does not actually specify 'information', but rather 'information technologies'. There appears to be an emphasis on physical assets in Australia's definition. The reality is that physical devices can be protected, but information in transit can be compromised. The most critical asset is the information conveyed by devices. It would seem more prudent to include a higher-level definition, if only for items declared or prescribed, such as that of the US DHS, as this provides the required flexibility to define criticality more holistically.

Furthermore, the list of critical sectors gives the impression of only relating to the private sector. It is worth considering whether the Act should also apply to those elements of the public sector, Federal, State or Territory, that are critical, such as Emergency Services.

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

No, see above.

Australia's definition does not specifically define information as critical, appearing to focus too exclusively on physical assets. The physical systems are important because they distribute information.

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?

The foundational message of the Consultation Paper could be interpreted to infer that interdependency and consequence are only relevant to the determination of the national significance subclass. Sapien does not believe that is intended, as it should also be used to identify other classes of critical infrastructure entities.

Given the increasing focus on diversity of supply, self-sufficiency, sovereignty, and the need for greater confidence in Australia's supply chains, manufacturing capability should be prioritised in relation to its effect on assessments of criticality. Therefore, 'deficiency' and

'uniqueness' should become measures for prioritising a critical entity that either needs to be protected or developed. One high profile recent example is the need for Australian companies to quickly retool to produce adequate supplies of appropriate PPE for Australia during the COVID19 pandemic.

The two factors of interdependency and consequence are a good way of considering criticality. As an addition to interdependency, the terms 'cascade' and 'compounding effects' should be used to describe the direct and indirect flow on impacts.

A mapping exercise would be a valuable tool to illuminate supply chain processes, providing insight into the top-level entity and also the nature of the underlying supply chains. Additionally, it is important that the Commonwealth is involved in this mapping and that it is based upon the impact on Australians, not just on the entity itself.

It is important to consider in the consequence and interdependency relationship, the impact on timeframe of the cascade of effect. For critical infrastructure that services the front line directly, an immediate impact of an outage of that infrastructure can have a rapid adverse effect on dependent services.

This interdependency can be more subtle and potentially delayed or even less visible due to a time lag or ripple effect in the supply chain. For example, it may be back end dependent, such that a failure in an overseas manufacturing portion of a supply chain does not become visible as an issue for some time later. Understanding such dependencies, especially with spare parts, becomes a very important overall map to track.

Similarly, the supply chain threat exists through strategically patient insertion attacks, where potentially malicious operators deliberately insert hardware and software behaviours, physical weaknesses or exploitable placements, into a supply chain expanding the attack surface exponentially.

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

Sapien's specialty focus is in the Operational Technology (OT) cybersecurity domain.

Sapien provides a unique convergence and visibility of why our clients seek to apply protection to their critical infrastructure, and how Sapien then translates potential cybersecurity threats through a number of attack vectors of potentially malicious operators/actors. Sapien learns what the customer deems critical to protect and why. Client's may not know nor understand the precise nature of the cybersecurity threat, but that is Sapien's expertise.

There are a range of common threats present in the contemporary cybersecurity landscape that we routinely prepare for such as: phishing attacks, malware and ransomware attacks, Denial of Service attacks, and data spills / breaches.

Sapien also prepares for those threats that may target our clients in the critical infrastructure arena, including Advanced Persistence Threat activity, ransomware attacks, and data breaches. As a business, Sapien has been successful in protecting our clients and operations from such threats, but we are fully aware that in today's scenario, no business, especially our own, can afford complacency and think themselves or their customers safe. In addition, we ensure that we maintain the physical security of our staff and assets and prepare for man-made and natural threats. The onset of the global pandemic required our business to rapidly adapt to an appropriate business model that allowed us to continue to operate at full capacity, while mitigating the significant risks to our staff and operations that the Covid19 threat poses.

Preparing for all contingencies is an ongoing imperative, and plans need to be responsive and adaptable to meet the need, particularly in rapidly evolving circumstances.

As well, this Consultation Paper should consider the rapid onset of the pandemic as a threat for a business to adapt to in the context of changing the business model. Preparing for all contingencies is a challenge and plans need to be adapted to meet the need.

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

Fundamentally, criticality can be based upon the loss of information and services that our society relies upon. However, such a simplistic approach might lead us to focus only on the denial of such a need (for example, the unavailability of a water source, certain foods, fuel) but not to consider more malicious impacts, such as the poisoning of or other weaponisation of staple and essential items.

The criteria described in the Paper are reasonable. Whereas the Paper acknowledges that the criteria may need to be sector specific, it might also note that the threats will vary across sectors and recognise that appreciating plausible threats and consequences is not a simple process.

Australia's critical infrastructure could be mapped to establish critical points of potential vulnerability resulting from different challenges. For example, the early stages of the current pandemic established critical points of vulnerability and failure around reliance on long and unstable international supply chains and highlighted the limited ability of Australian manufacturing to fill critical shortages (e.g. PPE). Criticality should be assessed against a range of critical events. Another example would be lack of availability of critical firefighting platforms, such as specialist helicopters for our emergency services organisations, as these are leased from the northern hemisphere. Increasingly overlapping fire seasons between the northern and southern hemispheres may lead to the need for Australia to develop new arrangements.

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

National significance can depend on the context of the threat. It is important to appreciate that the distinction appears purely on the basis that systems of national significance would be subject to enhanced cybersecurity obligations. In this regard, the key to this classification is identifying critical infrastructure that could have a substantial adverse impact on our society through the conduct of a cyberattack/exploitation.

Businesses should be advised what the Government considers to be a system of national significance. Currently we only have the statement that these are a subset of Australia's critical infrastructure that have the highest levels of criticality. Determining what falls into this category can be subjective and will differ for each respondent depending on the nature of threat, vulnerability scenarios, and their assessment of what is most critical to them.

We need a clear definition of what is a system of national significance for the Government with examples and rationale for why these are considered systems of national significance.

3. Government-Critical Infrastructure collaboration to support uplift

3.1 Response by Sapien

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

The Trusted Information Sharing Network (TISN) was initially successful because of the exchange of information and the trust between members of the TISN and government. Trust and meaningful exchange of information are integral to the success of a revised TISN. It requires both.

As there is significant cost associated with an organisation supporting its own membership of the TISN (staff time, travel etc), there needs to be tangible return on that investment for TISN members to participate. Specific areas of work to increase resilience in support of the Strategy should be developed. Consider, for example, the ability to use higher level principles developed from this work to assist smaller non-member organisations to increase their own resilience.

Improvements in risk management processes, accounting for plausible threats, as well as ensuring Board accountability, are important reforms.

Consideration should be given to who is the most appropriate representative to attend from each TISN organisation. This could be different based on the nature of the discussion.

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

Which entities are to be included should be informed by government's understanding of the national critical infrastructure community and which organisations are most relevant based upon an assessment of criticality and importance to the nation.

A few potential aspects to consider on how to interact most effectively with a revised TISN model could include:

- An operational information exchange model for the TISN rather than solely a policy/planning focus, with both virtual and physical meetings as required
- Representation from participating organisations should be drawn from relevant disciplines and positions, based on the discussion to be held at meetings (timely advance warning to TISN organisations would ensure the most appropriate representation)
- Multisectoral TISN meetings rather than sectoral meetings to facilitate cross sectoral information exchanges and sharing of constantly changing operational cyber security threat and incident information. This sharing of information can be used to recognise and defeat cyber threats as the threats and incidents constantly evolve.
- State government and state law enforcement representation should be encouraged at these meetings to ensure visibility, but also to ensure effective working relationships are in place to facilitate cooperation during serious cyber incidents.
- Information exchanges supported by online cooperation and collaboration would provide mutual benefit for all members, by enabling the resolution of incidents as they occur.

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?**

   Hold multi-sectoral meetings in addition to sectoral meetings like the TISN. For example, no bank can function without its telecommunications provider, energy provider, water provider etc. Increasing understanding across all those organisations about the cyber threats observed and experienced and what effects were being experienced will increase the resilience of entire chains. No sector is immune to the cyber threats that are being experienced by other sectors.

   Assistance with supply chain illumination tools as well as in development/validation of potential threat scenarios and acceptable risk appetite.

4. Initiative 1: Positive Security Obligation

4.1 Response by Sapien

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

    The four outcomes are universally applicable across the sectors.

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

    The obligations specify categories of expectations, rather than minimum expectations. More work would need to go into specific sector and entity requirements before they could be considered as clear expectations.

    There is a risk of trying to standardise requirements across sectors. There would be specific requirements that would be specific to sectors

    Clearly, there is a risk of attempting to standardise requirements across sectors with different risk appetites. Rather than applying global, sector-wide obligations and expectations, a targeted mapping between defined entities, sectors and obligations would facilitate the development of specific requirements aligned to each sector. This would clearly identify minimum obligations dependant on each entity's classification.

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?**

    Perhaps the question should be, how to define obligations that would benefit organisations struggling with the implementation of a cybersecurity solution to protect their operations?

    By providing clear expectations, entities would be able to define required budget and resourcing to meet minimum obligations, rather than the current scenario where solutions are deployed that are not fit for purpose. This will mean the total cost of ownership would be reduced and the timeline to reach an appropriate cybersecurity maturity would be obtained.

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

It is reasonable that an organisation should take on costs associated with obligations and mitigations required to address plausible risks. In that way a total cost approach that accounts for prospective losses of adverse events is best practice. It is just as reasonable that organisations may need to either recoup such costs from clients or government.

Two difficult areas for negotiation in this process may be mitigation of plausible versus probable risks; and mitigation of risks that impact on the client rather than the organisation.

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?

See above; N/A.

5. Regulators

5.1 Response by Sapien

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

Subject to implementation. Ideally, regulatory models should be complementary.

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?

Firstly, in the international landscape, precedence has been set by other nations. For example, in the US standards have been applied to critical infrastructure cyber security frameworks for a number of years.

Given the importance of Australia's critical infrastructure, we should capitalise on this opportunity to provide owners and operators of Operational Technology guidance on their evolving risk exposure. This combined with the recent global pandemic highlights the risk to the nation when our dependence on other countries is integral to ongoing sustainable provision of essential services and products. Choosing to use international products and services over sovereign capability may introduce significant levels of risk and threat for organisations, particularly in relation to times of heightened tensions.

The regulator should be tasked with clearly articulating the expected national and international cyber security standards against which critical infrastructure entities must comply. This should also include standards on a workplace cyber culture and workforce training and awareness.

The regulator will not achieve the aim of protecting entities from 'all hazards' unless it is mapped and measured against national and international standards and applied to information technology, operational technology, Internet of Things and supply chains.

Clarity of standards allow Boards, owners, and operators to assess objectively their compliance with regulatory obligations. 'Best practice guidelines' do not. Standardisation of governance processes and associated accountability ensures that decisions within critical infrastructure organisations focus on deploying the right cybersecurity solution, not 'a' solution.

Sapien believe that the growth of a sovereign domestic cyber security capability and the protection of Australia's critical infrastructure are foundational to Australia's national interest now and in the future, and that they should be supported and facilitated.

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?

See 16 Above.

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

Appropriate briefings from Government agencies about specific threats, and good levels of relationship between regulators and those agencies to ensure that information is made available to regulators as it becomes available.

Risk management consistency, and consistency of cross-sector dependencies, and clarity about risk appetite (including consideration of plausibility vs probability).

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

Given the reporting requirements and potential punitive measures of the new regulatory environment, Boards, owners and operators of critical infrastructure entities will seek assurance from external cyber security auditors about their compliance with the Positive Security Obligation, in the much same way they seek assurance from external accounting auditors for their financial statements.

Government should consider mechanisms for identifying trusted Australian industry organisations to assist critical infrastructure. This would eliminate much of the trial and error approach for critical infrastructure organisations as they seek industry assistance on this matter. It would also assist the Australian Cyber Security Centre to build a trusted list of providers to undertake such work.

To ensure the integrity of the assurance and reporting process, the Government needs to develop an accreditation system for cyber security experts, as a matter of urgency.

The accreditation system needs to:

- be nationally recognised
- only recognise relevant cyber security qualifications from nationally recognised, accredited vocational or tertiary institutions
- be overseen by one or two nationally recognised professional associations
- only recognise prior learning that has been assessed by the professional associations, and
- be modelled on the approach used for financial auditors.

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?

A similar scheme would partially address the risk of insider threats from a human perspective within a specific sector. However, it would not account for human based insider risks within critical infrastructure associated supply chains. Further, additional sources of insider threat, posed by untrusted hardware and software would require additional guidance and controls, such as through the use of preferred suppliers of technology.

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

No.

6. Initiative 2: Enhanced Cyber Security Obligations

6.1 Response by Sapien

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

It is essential to have existing strong relationships that can be called upon as required rather than trying to build those active partnerships when threats emerge. In the absence of the CERT, that relationship should be with the Australian Cyber Security Centre.

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

Incident and threat information and how to mitigate them. Sharing in practical ways assists with better understanding of how to prepare and what to do. Sharing should be seen as two-way sharing. Government should not underestimate what it can learn from industry as some industry organisations have significant capabilities.

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?

Sapien's architecture was designed for the ease of sharing anonymised data and creating threat signatures within our client base. The expansion of Sapien's client base in critical infrastructure would inherently increase the visibility of attacks across key industry verticals and key areas of interest for Australia.

Sapien would be open to discussions with Government agencies on how we could best structure our contribution to a national threat picture.

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

Networks are increasingly interconnected such that it is very difficult for some organisations to determine what is their perimeter. Also, that factor is often overlooked as a source of vulnerability within organisations that can negate even the most significant perimeters.

Why focus only on the perimeter of critical networks? Perimeters are less relevant in the modern environment, where a cybersecurity strategy is founded on a combination on the 3 pillars of people, process and technology.

Traditionally, OT networks have been physically separated from Information Technology (IT) networks. However, with changing technologies and a drive towards data-driven and remote operations, the two technology environments are starting to interconnect. This interconnection is now widely known as the IT/OT convergence. This IT/OT convergence increases the cybersecurity challenges that are typically associated only with IT networks. OT data that is then accessible from these environments could include critical information such as pressures, temperatures, proximity levels, control signals and other sensor signals.

Remaining cognisant of today's modern networks, Sapien monitors traffic not just at the perimeter, but also meshes multiple technics to identify and track potential threats as they laterally move within the network. This approach forms part of the layered cybersecurity approach employed throughout the Sapien solution.

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

Trust is one potential barrier and that exists for all sources of information alerts (threat information). It is the nature of a security professional to constantly question the source and the veracity of the information.

Another barrier is requiring those receiving information to hold security clearance and providing them with classified security information. This makes it extremely difficult for individuals to act accordingly within their organisations to protect the organisation as they cannot disclose classified information to those working with them.

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

Within sector verticals, each organisation is different from every other, and therefore the content and approach to individual "playbooks" would differ for each organisation. In order to co-develop playbooks with Government that would provide value to organisations and consistency in Critical Infrastructure protection approaches across the sector, the fundamental elements of best practice across the expanded definition of Critical Infrastructure will need to be identified. The Government may consider co-developing a range of different generic procedural documents that embody the identified best practice principles, which could then be adapted for use by individual organisations. Ideally, playbooks should contain clear and repeatable steps that adhere to the fundamental best practice principles, regardless of the specific scenarios. Best practice principles should not only define essential playbook content, but also define the development, use, and review of playbooks. For example, playbooks are live documents that require regular testing and updating.

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

That it is only used for the purpose it was intended for, and that the purpose it was intended for is understood and agreed by both parties. Also, that the information is appropriately secured to ensure that it is not compromised.

Wherever possible that the information is anonymised in some form (for example, to a sector rather than an organisation). The exception may be for information around incident response, with tight controls around who has access to that information.

7. Initiative 3: Cyber assistance for entities

7.1 Response by Sapien

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

Actions to ensure national interest and security around critical infrastructure that may be at increased risk. In extreme situations it is appropriate for government to take direct action against an imminent cyber threat or incident which could impact adversely on Australia's national interest or sovereignty.

Note that some nations have the authority to temporarily take control of critical infrastructure under certain very serious cyber incident situations. The Netherlands is a good example of that in the past in relation to attacks on the telecommunications sector.

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?

Government on advice from the appropriate Ministers responsible for security agencies and agency heads, and the Attorney General.

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

A Commonwealth Office(r) with powers comparable to the Inspector General of Intelligence and Security.

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?

Government should be able to deploy the best cyber security capability available to it to disrupt perpetrators and to protect the national interest and Australian sovereignty.

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

The appropriate usual indemnities for Commonwealth officers and others when acting consistent with the law.

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

See answer to Q. 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?

Within critical infrastructure operations, Sapien acknowledges that not all equipment in the OT environment can be sovereign, and in some cases are supplied from non-trusted sources.

What should be of focus is the associated risk assessments that inform supply chain decisions, including investment decisions, as to how much assurance, resilience and sustainability is required in each part of the associated OT environment. However, what should be a priority is an increase of the sovereignty of cybersecurity capability to monitor, reduce the threat exposure and in turn mitigate supply chain risks.

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?

The danger would be in any misunderstanding between the parties on who took action because of specific information. Clarity of obligation and clarity of operational standards will be essential.

End of response.