September 16, 2020

Critical Infrastructure Reforms Group
Department of Home Affairs

Dear Sir/Madam,

Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

Leidos Australia welcomes the opportunity to make a submission to the Department of Home Affairs consultation. As a prime contractor in the Defence and Security sectors in Australia, the United States and the United Kingdom, we recognise the importance of both identifying and protecting critical infrastructure. Throughout history, and no more so than now during the COVID-19 pandemic, it is important to articulate those critical foundations for our country that are vital to our economy and security and the wellbeing of our citizens.

We have provided initial responses to the questions you have asked and look forward to more detailed discussions as you further develop reform proposals. Our responses are based on a long history of providing critical infrastructure and services in the Australian market, combined with similar experience in other countries. We are also an active member of the Australian Industry Group and have provided it with a copy of this submission.

One aspect that Leidos Australia would like to highlight is the dependency of Critical Infrastructure on a number of facets, an important one of which is cybersecurity. This submission is based on our feedback in regards to cybersecurity; however, we note that the implications for changes in legislation may be broader than just this focal point.

If you would like further clarification about the Leidos Australia submission, please do not hesitate to contact me ([redacted] or [redacted]) or my Vice President Corporate Affairs, Simon Carr ([redacted] or [redacted]).

Yours sincerely

[redacted]

Paul Chase
Chief Executive
Leidos Australia

Leidos Australia
ACN: 612 590 155
53 Wentworth Avenue
Kingston ACT 2604, Australia **P:** +61 2 6201 3501

Department of Home Affairs

PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE

RESPONSE TO CONSULTATION PAPER

16 September 2020

leidos

Table of Contents

Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
ASD	Australian Signals Directorate
AWS	Amazon Web Services
CI	Critical Infrastructure
DISP	Defence Industry Security Program
IS&GS	Information Systems and Global Solutions
ISM	Information Security Manual
JCSC	Joint Cyber Security Centres
NIST	National Institute of Standards and Technology
SME	Subject Matter Experts
SOC	Security Operations Centre
TISN	Trusted Information Sharing Network
US	United States

1 Overview

1.1 Sectors to be Considered

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 industry sectors listed in the consultation paper cover a wide range of Critical Infrastructure (CI) industries. The interconnections and interdependencies of many industries place criticality on adjacent industries as well. Logistics and supply chain would be expected to be included as an important part of Transport. Manufacturing Industries, especially those interacting with listed sectors such as Defence should also be considered. Leidos Australia recommends that critical services provided to all the CI be included with the sectors being considered. For example, Cybersecurity Operations Centres (SOCs) that support CIs should be included in the planning.

Leidos Australia recognises that, based on the definition provided of critical partners in the Defence Industry, we would be considered a CI.

1.2 Definition of Critical Infrastructure

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

> *The Australian Government's Critical Infrastructure Resilience Strategy currently defines critical infrastructure as: 'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.'*

To allow for changes in what determines infrastructure rather than specific explanations of each asset type, the current definition meets the purpose of setting the context of CI, but the definition could include the context of critical services provided to the CI.

1.3 Factors to be Considered when Identifying and Prioritising Critical Entities

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?*

A risk-based approach should be considered when identifying and prioritising critical entities and entity classes. This should include recoverability of the infrastructure to determine the overall consequence of compromise. Refer to Section 1.5 for factors in assessing criticality.

1.4 Common Threats

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

Leidos provides critical cyber operations services to CI and Federal Government agencies globally and has deep insight into cyber adversaries and threats. Common threats include:

- Phishing campaigns (and their derivatives, such as vishing and smishing) that cause the first line of ingress into an organisation's network through broad campaigns, as well as spear phishing, where targets are socially engineered to bolster the validity of the attack

- Direct overt hacking of systems through complex attack forms, which are at machine speed making identification, response and recovery much more difficult if underprepared
- Insider threats, such as unintentional consequences of users' limited awareness, business processes and malicious insiders.

Leidos Australia has a strong heritage in the application of risk-based, including threat-based, security controls to support ourselves and our customers. Our progenitor organisation, Lockheed Martin IS&GS, developed the Cyber Kill Chain, which is now owned and continually developed by Leidos to better frame threats against organisations, and Leidos Australia continues to use this framework to support our cyber security controls and preparedness activities.

In addition, we recognise that the protection of critical infrastructure and systems of national significance needs to consider more than cyber risks. The recent bushfires and floods and the COVID-19 pandemic highlight the risk to highly interconnected supply chains and capabilities across the country and across the globe. It is necessary to consider risks from all sources (for example, cyber, natural disasters, pandemics, and state and non-state based actions).

As an organisation that is heavily interconnected with a local and global ecosystem of customers and suppliers/partners, Leidos Australia frequently reviews a broad spectrum of threats, our risk exposure and appropriate mechanisms to mitigate those risks. Part of this assessment and mitigation is ongoing collaboration with government on mechanisms to sustain and build resiliency in our operations.

1.5 Assessing Criticality

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

To attain and continually strengthen cyber resilience, it is important to constantly assess risks in a systematic approach of threats, intent, probabilities and consequences to determine which current or future mitigation controls will be effective. To assess criticality, the same methodology should be applied – employ a risk-based approach to potential CI entities to ensure the overall factors of consequence to the nation are considered. For instance, telecommunications providers have the ability to recover and continue providing services through high-availability and redundancy, therefore their ability to continue critical services positively affects the reduction of the consequence over time. Conversely, water supply infrastructure could take longer to recover, which would have a profound impact on the nation in many ways and therefore would have a more negative effect on the consequence over time. Other factors as outlined in the consequences should have a risk applied to ensure that a holistic view of the CI is considered for assessment, classification and therefore ongoing certification.

1.6 Owners and Operators of Systems of National Significance

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

Ideally, the most critical assets would be government owned; however, with privatisation and the total cost of ownership, the asset could be co-owned by government and industry if the CI is of high national interest. This could include a percentage of ownership by foreign entities; however, the Australian majority owner would need autonomy to make decisions in the national interest before that of the foreign entity.

Outside fiscal considerations, information sharing with the foreign entity would need to be restricted to ensure that critical information is protected. As in traditional outsourcing, the risk is on Australia as a nation, and therefore it is paramount that the nation, or the Australian majority owned entity retains a level of influence and control.

The operation of systems should be led by industry; however, with the level of criticality, ideally it should be done by a collaboration with government similar to Defence Industries to ensure that fit and proper facilities, technologies, processes and resources are tenured. In particular, critical activities such as security auditing, monitoring and response supporting the CI (both physical and logical security) should be undertaken within our national borders. This is to reduce any risk of influence, tampering or circumvention of critical controls, allowing the CI to maintain situational awareness and command and control activities to mitigate, respond to, recover from and forensically investigate any security incident. Industry-based local security operations centres would be best positioned to provide this service to drive economies of scale as well as the ability to leverage secure information across all CIs to create optimal situational awareness supporting national interests. Service Provider's to Government must have CI experience, accreditation and vetting to ensure that facilities and resources meet Australian Government expectations of fit for purpose. For example, Service Provider's facilities and resources are considered an extension of Commonwealth capabilities, which also benefits the Commonwealth, by providing better access for agencies who may engage directly, to better support the CI.

If any foreign entities are involved in CI through ownership of local entities or service provision to the CI, it is imperative that Australian legislation is complied with including foreign ownership legislation. An example of such compliance is Leidos Australia's licence to operate based on vetting of sites, processes, technologies and personnel who have access to protected information and protected sites.

2 Government-critical Infrastructure Collaboration to Support Uplift

2.1 Revision of TISN and Critical Infrastructure Resilience Strategy to support reforms

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

Should reforms be implemented with the regulatory obligations defined, it will be important that the Trusted Information Sharing Network (TISN) and resilience strategy align to the overall obligations. This would provide an approach of commonality (the regulation) as the foundational aspect of CI. Given that the TISN and resilience strategy use a risk-based approach, it is important that the overall regulation supports this methodology to determine CI category according to risk to national interest.

2.2 TISN Model

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

The model, if altered, should include all CI sector representation, including critical Industry service providers, to ensure value input and cross collaboration of information sharing where appropriate.

2.3 Focus Activities

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?*

Information sharing is critical to a sound security posture and the Australian Government has a critical role in this. Notwithstanding classified information, the ability to inform CIs of current and

emerging threats and risks will assist the CIs to a better security posture, as well as having a broader view to assess related risks in sector and cross sector, in turn supporting the customers and the outcomes of the CIs. Focus should be placed on providing this information in the right format for the audience, whether through a structured or unstructured format, to support automated operations and identification of common threats. Information also should include how each of the industries in the sector are complying with security recommendations, or at what level of maturity they are, to allow other like entities to baseline their capability as well as provide insight into other CI industries.

3 Initiative 1: Positive Security Obligation

3.1 Principles-based Outcomes

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

Having principles-based outcomes ensures that the CI and subsequent service providers are able to apply controls, processes and technologies to the principles without restriction. For example, Leidos Australia bases our principles-based methodologies that are used internally and to support projects on the Cyber Kill Chain methodology and NIST Risk Management Framework and controls, which are attributable and mapped to Commonwealth Information Security Manual (ISM) and Australian Signals Directorate (ASD) mitigation strategies. The use of these principles avoids implementing a 'compliance' or checkbox approach to security and allows security to be implemented in a tailored and relevant fashion, ensuring that it is an enabler to business. Our approach also allows us to use standard controls, while being able to map to principles-based outcomes making it easier for each CI to provide functional mapping of controls that meet the principal-based outcomes.

3.2 Balancing Security Obligations

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

Security obligations that are attributable to principles provide the ability to have a mandated baseline expectation allowing for consideration of an organisation's capability and special requirements. This gives the Commonwealth, CIs and service providers a predictable level of obligations that are required at minimum. Further, leveraging a risk-based approach on the CI allows for the effective threat and vulnerability assessment of the risks and controls to determine their individual risk rating and application of customised control obligations that will reduce the risk. As the CI should be measured on the risk of consequence, any customisable controls and outcomes can be easily applied through having the standard baseline and further control effectiveness that is bespoke to the risk and CI. There is no guarantee that an organisation will never face a successful cyber intrusion, and thus the security incident and remediation process should be measured to identify deficiencies in the case of a compromise. The benefit of continual improvement extends to a standardised approach that tends to better levels of assurance as a whole-of-CI view, as well as adaptation of customisation where needed that could be leveraged as an industry.

3.3 Impact of Meeting Principles

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?

Leidos Australia's facilities, technologies, people and processes are aligned with the Defence Security Principles Framework and the ISM, which provides a clear expectation of capability that is risk based, and verifiable. Having a standard set of expectations in accordance with the ISM gives CIs the ability

to better select and partner with service providers such as Leidos Australia, given the verifiable level of compatibility to expectations and obligations and a clear focus on appropriate security implementations.

CIs and service providers that do not meet the level of expectations would require an uplift in maturity capability that could potentially increase time and cost of compliance if very specific mandated obligations were set out. Leidos Australia also recognises our and the country's reliance on subject matter experts (SMEs), and their difficulty in achieving innovation and improving Australia's desired national posture when faced with an increased barrier to entry into the market. However, given the level of national importance of the CIs, SMEs should have to meet set principle-based objectives to achieve a licence to operate, ensuring a baseline of expectations is met and verified.

3.4 Cost of Meeting New Obligations

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

Like the Banking and Finance sector, as an entity, there is a requirement under the prudential authority to certify and hold a licence to operate. Therefore the cost must not be a consideration in achieving this, otherwise risky processes, behaviours and capabilities could impact the nation. To alleviate the cost, a maturity roadmap based on the risk profile of the CI should be developed to ensure that the risks are mitigated appropriately over an accepted timeframe. Cost considerations also need to drive the stringency of the requirements: if costs become prohibitive industry could be deterred from collaborating or could pass costs on throughout the supply chain which includes potential cost increases to the consumer.

3.5 Sectors Impacted by the Security Obligations

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?

Defence Industry is a very good example where any organisation supporting defence, like Leidos Australia need be a member of and comply with the Defence Industry Security Program (DISP). The DISP requires members to achieve a level of assurance in cyber and physical security which comes at a cost to the organisation of developing and managing control obligations. This program is critical to enable Defence Industry to interact with and provide services to Defence which should be considered with the CI sector. Dependant on the level of security maturity, an organisation may need to enhance their security posture in order to operate in this environment under the DISP. The DISP framework provides a clear obligation which ensures a level of trust for interaction and support. It is important that the DISP considerations are de-conflicted with the regulatory and other obligations that are proposed by this process.

4 Regulatory Model

4.1 Regulatory Model Impacts on Existing Oversight Requirements

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

Baseline expectations of a regulatory model help avoid duplication, which then also provide a reference point of requirements in line with other oversight requirements making it easier for each CI to meet multiple regulations. This is imperative for assets and services that support the national interest as it empowers the Commonwealth, CIs and service providers with a common set of standards based on their risk profile. Therefore, assurance and insights of national interest can be

holistically viewed, managed and mitigated more effectively. A standard that is repeatable also allows each of the CIs and their service providers to measure and manage their capability maturity based on an industry benchmark giving a clear measurement of their current and future state of compliance and uplift where needed based in an industry road map of expected state.

4.2 Sector Regulator Strategies

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?

A series of self-assessment checklists for internal audit and project planning and assistance for the CI and service providers that are not at an acceptable maturity level would be of benefit to allow for a definitive maturity plan based on their current state. This in turn would benefit the regulator by developing insight into the overall sectors and providing a holistic approach to supporting the uplift in maturity.

Information sharing at the sector level, as discussed in regards to the TISN, is also critical to enabling the appropriate decisions to be made to implement security controls in regards to the sector. Although organisations' views differ on the vulnerabilities in their systems, this common threat picture will enable organisations in the sector to determine their risk profiles.

4.3 Organisations Best Placed to Perform Regulatory Roles

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?

Within the DISP, Defence has a pseudo-regulatory body: the Defence Security and Vetting Service. This body could be given more powers as part of the changes in regulation in order to support Industry partners and the CI. An alternative is to establish all cyber security regulatory approval through ASD or the Australian Cyber Security Centre who perform like type activities, have the requisite experience and focus on protection. This alternative approach could also lead to better information sharing, given that inter-departmental collaboration would ensure that information is captured, analysed and disseminated in a more timely manner.

4.4 Support for Sector Regulators

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

For the sector to continue to mature, change management and education are paramount. This could include general information sharing that all CIs could draw on as part of an ongoing continual improvement program. Further, the information held by the regulator would provide greater insight into how each CI and service provider is tracking compared with its peers, without giving away competitive information. This type of report would be tailored to each entity to allow for understanding of importance based on their risk classification, but also for the ability to help build business cases of investment aligned to a measurable maturity path and industry peers.

4.5 Government Support for Critical Infrastructure

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

Leidos Australia ensures that situational awareness improves our organisation's security posture through using intelligence-led information for better decision making to identify, assess and mitigate security risks. Information sharing of incidents and risks is paramount to the overall resilience of the CI sector and it is where service providers such as Leidos Australia can make a positive difference, given that we manage our own cyber risks as well as those of our Australian Government customers, in both unclassified and controlled environments. Information sharing where applicable from Commonwealth entities would further improve the overall maturity of the CI sector through improved situational awareness of current and emerging threats.

4.6 Models to Mitigate the Risk of Insider Threats

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?

Given the national importance of the data and systems, CI employees, contractors and service providers should undergo stringent vetting processes in alignment with the Protective Security Policy Framework and Australian Government Security Vetting Agency clearances. These processes have ensured that Service Providers are able to provide critical services to Commonwealth entities, including access to and sharing of information at protected level, which is paramount to the successful provision of cybersecurity services.

4.7 Comments on PSO

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

Leidos Australia does not have comments to make regarding the Positive Security Obligation at this time.

5 Initiative 2: Enhanced Cyber Security Obligations

5.1 Activities to Proactively Identify and Remediate Cyber Vulnerabilities

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

Being prepared for cyber risks and vulnerabilities is an ongoing effort due to the ever-changing threats and methods leveraged by threat actors. Based on Leidos Australia's experience, continued monitoring and assessment of cybersecurity risks and subsequent vulnerabilities strengthen an organisation's security posture. We use the PICERL (Prepare, Identify, Contain, Eradicate, Remediate and Lessons Learnt) methodology developed by the SANS Institute to combat security incidents, which in turn supports an understanding of the threats and vulnerabilities to a system. These are then analysed: threats through the Cyber Kill Chain and vulnerabilities through organisation-specific policies and processes to gain an overall understanding of system-specific threats and vulnerabilities. Further, continued vigilance is increased through user or entity awareness of the risks that should be part of continued change management to ensure resilience at the user or entity level. This must form part of the industry mindset to 'proactively think cyber risk' as part of business as usual rather than a reactive approach where risks have been realised and incidents occurred. When an incident has

occurred, the lessons learned through a continual improvement program bolster preparatory activities and increase cyber maturity.

5.2 Information Sharing

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

Cyber threats and incidents impact many organisations at the one time. Sharing of information of threats, vulnerabilities and actions provides a higher level of situational awareness for all organisations to allow them to assess the risk according to their risk security posture, framework and appetite to allow better mitigation.

Information sharing by government sources where reasonable would benefit the sector as a whole, similar to enterprise environments like the financial services ISAC. This would include information of the threat actors currently targeting Australia and our national interest and their intent, the types of methods employed and vulnerabilities being exposed by the threat actors, and remedial activities that could be used to reduce the risk of exposure and consequences.

Leidos Australia is a member of the Joint Cyber Security Centres (JCSC) Partner Program, and information sharing through this program is already yielding benefits in supporting our proactive defence measures, our application of risk-based security controls to new programs, and our customers. An expansion of this program and a specific focus on critical infrastructure would be welcomed.

The importance of sectors members sharing intelligence information with the sector as a whole cannot be understated. One of the reasons this has not occurred with great success is the lack of a framework to support it, as well as a perceived conflict of interest in sharing information with competitors. The Australian Government could help alleviate these issues by stating clear frameworks and policies that could be agreed by sector participants in order to share information among themselves. A good example is the Financial Services Information Sharing and Analysis Centre (FS-ISAC), where information sharing of cyber risks in the interests of the industry outweighs the potential consequence of competitive advantage.

5.3 Leidos Australia Contributions to a Threat Picture

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?

As a provider of critical cybersecurity services to the Commonwealth and United States entities, Leidos Australia draws on this information to ensure the organisations we support are better prepared through analysis and replication of risk mediation where possible. Our collaborations with global vendors that provide technological solutions to support our capabilities increases the value of security postures to all the entities we support. Where publicly available, with no impact on customer obligations and expectations, and no requirement to reveal intellectual property, a source group of information would be beneficial and supported by Leidos Australia.

5.4 Methods to Identify Perimeter Vulnerabilities

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

At Leidos Australia, we believe that the perimeter provides a critical first line of defence to reduce ingress points for the attackers. However, our experience also tells us that perimeter-focused security protection is no longer enough to provide assurance over a system. It is important for organisations to employ a defence in-depth approach to security, ensuring that security controls have relevant crossover to counter threats that may be able to bypass controls. This also requires a holistic picture of a system to ascertain an organisation's true vulnerabilities and risks, from the perimeter to the core.

To protect the integrity of critical perimeters, continual monitoring and testing of vulnerabilities should include:

a. Firewalls that ensure appropriate levels of ingress into the network through predefined rules that also must include geolocation restrictions for critical environments.
b. Vulnerability scanning of firewalls, networks, systems and services, for example, Amazon Web Services (AWS), Google, Microsoft Azure/Office 365, and websites to continually identify areas of weakness for remediation.
c. Vulnerability testing and education of the end users at the final line of defence to ensure the human perimeter is vigilant in all their activities, processes and interactions.

The egress perimeter also requires the same level of insight to ensure and reduce the opportunity of insider threats.

5.5 Barriers to Acting on Information Alerts

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

The value of Leidos Australia's cyber capabilities rests in experienced resources focused on the mitigation of cyber risks. Therefore, we see the barriers for CIs as being under-resourced with cybersecurity skills. In some cases where there are limited resources, organisations generally do not have enough resources, experience or bandwidth to act on the identification, management of incidents and remediation cyber risks, and therefore cannot reduce the exposure. The lack of defined cybersecurity processes in an organisation can also impair the preparation, monitoring and remediation of risks.

5.6 Playbooks

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

Although playbooks add value to the initial preparation and remediation of cyber risk mitigation, these need to be continually assessed and updated to ensure they are fit for purpose, given the rate of change of the threat landscape. A potential barrier to co-developing playbooks with Government would be the continued effort of efficacy validation and development of new playbooks as the need arises from budgeting, resourcing and educating perspectives.

5.7 Information Safeguards and Assurances

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

Information sharing and handling should be conducted through established information classification protocols such as the Australian Government Classification system and traffic light protocol. Therefore, assurances from all parties relate to how information shall be received, handled and stored in the interest of all parties concerned.

6 Initiative 3: Cyber Assistance for Entities

6.1 Government Direct Action Triggers and Limits

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

In the same approach of other cyber incidents that have occurred (for example, the Australian National University breach), the Commonwealth and its agencies should be able to take direct and indirect action based on a predefined level of risk consequence. This should be predefined as to roles, responsibilities and actions to ensure the government and CI are actively collaborating and not impacting each required outcome. For example, when an incident occurs, a government may be required to conduct offensive cyber actions to identify and counteract the threat actors. Because this could have diplomatic or economic consequences, it should be directed or led by the relevant government agency. Any offensive activity should only be undertaken by a government agency under extreme circumstances where a significant amount of evidence is identified in order to focus on the adversarial intent and to limit the consequences.

6.2 Emergency Declarations

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?

Based on the consequential risk and potential source of the threat actors, the government should have the power of emergency declaration through advice and information from the impacted CI. There should be clear processes and decision points to ensure that such information and advice from the CI to the relative agency is timely and in a format to reduce the decision time to declare.

6.3 Government Oversight

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

Should a predefined plan and decision markers be approved and implemented, and coupled of the fact of the consequential impact of the incident adversely dependant on whether the threat actor is state or criminal based be the Inspector General's officers or relative law enforcement dependant where the criminal based attack originates from.

6.4 Government Disruption of Cyber Attacks

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?

As outlined in Section 1.6 and Section 6.1, there should be predefined markers for effective and fast decision-making processes to ensure that the Commonwealth is responsive to actions that require command and control of the situation. Any response must take into account that the level of consequence differs between state-based and criminal-based attacks, and ensure that it does not affect the nation's best interests.

6.5 Legal Protections for Emergency Actions

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

Leidos Australia recognises that legal protections for all parties will be required but their nature and depth will be highly complex. There exists an interrelated framework of national security and regulatory legislation in this area; any further changes to their scope will have larger implications. This question requires greater consideration and context before we can respond, but we would welcome the opportunity to discuss it further.

6.6 Safeguards and Oversight Measures for Emergency Powers

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

Planning, agreement (including contractual) and ongoing testing/simulation should ensure that the powers are defined and suitable. Through planning and agreement, clear roles, responsibilities and accountability must be clearly documented to not only assure safeguards, but ensure that the actions and accountabilities are in the interest of the nation.

6.7 Risks to Industry

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?

Each CI, through the guidance of policy and regulation, must conduct an assessment of enterprise and cyber risks to determine their acceptance and or mitigation of identified risks. As outlined in Section 1.6, this is more critical if there is full or part foreign investment in or ownership of the CI.

6.8 Obligations and Assistance in Protecting Critical Infrastructure

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?

As outlined in Section 1.6 , given the level of national significance, the overall accountability of the risk is with the Australian Government. However, like Leidos Australia as a critical service provider, private sector suppliers must share the accountability of mitigation and provide accreditation of the mitigation strategies through enterprise and cyber risk frameworks. This in effect increases collaboration through sharing of the risk as well as ongoing trust and further opportunity to collaborate. Risk in change should be identified, analysed, assessed and then communicated by the government to the CIs based on the ownership of the risk and consequence to national interest.