BizCarta
Making Security Work As 1
Security Consulting Technology Integration Managed Services
ABN: 78636530900 | Ph: +61 466 216 443

15th September 2020,

Response to Consultation paper titled "Protecting Critical Infrastructure and Systems of national Significance"

BizCarta Technologies Australia Pty Ltd appreciates the opportunity presented to provide views on the questions raised on the aforementioned consultation paper. We feel certain questions are already addressed in the consultation paper and we do not intent to add any further on it. Questions that we intend to answer are captured in the subsequent section of this document.

Bizcarta is a Cyber Security Consultancy and managed service provider with presence in and out of Australia. This gives us a global understanding of approach taken over Cyber Security. The difference in approach can be seen in the thought process put in drafting various regulatory compliances.

BIZCARTA
MAKING SECURITY WORK AS 1
Security Consulting Technology Integration Managed Services
ABN: 78636530900 | Ph: +61 466 216 443

Views:

This tables captures our views corresponding to the questions. No# depicts the hierarchical number of the question in the consultation paper.

No#	Question	View
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 and functions are captured well. What we feel missed are the enablers of these functions. A very good example would be the service that offers manpower. Direct organisation employees undergo rigorous background checks, but what governs the manpower providers.
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?	Entities must be covered in a much broader manner with a deeper understanding of its use and impact on failure. Seldom the interconnecting aspect is considered while calculating the risk. A function might be trivial in nature, but it would be in close proximity or may even be connected to a quintessential service. Segregation of functions must not only be based on criticality and sensitivity of the data it holds. Must also be based on it collective impact.
4	What are the common threats you routinely prepare for and those you have faced/experienced as a business?	Unlike any private organisation Government data can result in loss of life. Eg:- Gun's Registration, Witness Protection, National Strategy and so on. As every government agency has one or the other way to connect to each other the attack vector is very large. A well planned and patiently executed attack is possible as the data is worth that much. No stones should be ever left unturned under any circumstances.
5	How should criticality be assessed to ensure the most important entities are covered by the framework?	Criticality of an entity must not confine to the criticality of the data it holds but also to other entities to which it can be pivoted to. One common thing with Government is that there are many legacy functions. Even though all are moving to cloud, replacing them from one box to another without changing anything is not modernisation. They still are legacy. With legacy you bring a lot of risk. These risks tend to get overlooked as they may not

		be sensitive data. What we miss is the fact that these risks would dilute the newly built cloud or data centre with all new tools and toys. So, criticality must be assessed in totality. If that cannot be done, then functionalities must be segregated with robust segmentations.
6	Which entities would you expect to be owners and operators of systems of national significance?	Anything related to National Significance must be owned and operated by Federal Government with need to know basis data sharing with State Government
7	How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	If major recent incidents are considered it is evident that the cause of it is not just technical shortcomings, but also awareness of the users too. A reformed knowledge sharing of common threat methods would increase the awareness of all users. This the human element can be reduced which will reduce the overall vulnerability many folds.
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?	Security awareness in general must be mandated to all users of the system. Critical or otherwise. It would be hard to pinpoint the area from where the attack may happen.
11	Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	Security requirement must have a robust risk assessment that caters for all the risk aspect covering the entity it it's totality
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?	Upliftment of legacy systems to at least come near to the modern ways of working. With that a MAJOR chunk of vulnerabilities and risk gets removed.
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	Regulatory body must consist of Government entities and external or non-government representations. Their work must be evaluated by a 3rd party

BIZCARTA
MAKING SECURITY WORK AS 1
Security Consulting Technology Integration Managed Services
ABN: 78636530900 | Ph: +61 466 216 443

27	What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?	If and when there is an attack on the Government functionalities it must be considered as a war (not in literal sense, but in the context of urgent responses). Relevant response team must be aware of their roles that needs to be performed that would include from waking people from sleep to cutting down the power lines with an axe. These playbooks must be re-visited on a periodic manner through workshops with the relevant responsible.
28	What safeguards or assurances would you expect to see for information provided to Government?	Confidentiality would be the most important factor. There are various forms of information that can be provided to the Government. It ranges from insider abuse to a planned terrorist activity. Either of that is life threatening to the whistle blower. Their safety and closure must be the most important aspect that we would want to see.
29	In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	Government must be able to take extreme action in case of national interest. Actions like a nation-wide media, internet blackout, up to a decent curfew is 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?	The Prime Minister must be the only person who should make such a declaration. He must consult with his advisor from all aspects of the nation, like defence, economics, human welfare and tele communications.
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?	Irrespective of our attacker or their position we must not cross the line. Our sole requirement is the safety of our people by ensuring continuity of our services to the people. Offense is not the best defence all the time.

BIZCARTA
MAKING SECURITY WORK AS 1
Security Consulting Technology Integration Managed Services
ABN: 78636530900 | Ph: +61 466 216 443

Other points that we think as important are:

- Before every targeted attack there are always chatter in the deep and dark web. Monitoring the deep and dark web for any such references would be a very good aspect to be prepared.
- There are many ways to identify vulnerabilities within the premises (cloud or on premise) but there is not much thought given to identify exposed devices.

- 3rd Party or inhouse government organisation must perform these deep and dark web sweeps and find the presence of exposed assets and share that intel with respective organisations.
- This will ensure that we would know our faults sooner than our attacker.

Being a Cyber Security Consultancy, we are happy to demonstrate the capability and cost that would in concur for periodic activity can be discussed.

Yours Sincerely,

[redacted]

AB Nair
Director
BizCarta Technologies Australia Pty Ltd