Protecting Critical Infrastructure and Systems of National Significance

Alive Information:

Alive Information, a business of Australian Engineering Exports P/L, has been in business for more than twenty five years and has a history of introducing new technologies in industries and workplaces usually leading a group.   Many of these projects have used risk as the pivot point for implementing a strong argument.

A submission was presented to Aust Cyber on the development of Key Performance Indicators and Key Risk Indicators for the evolving energy industry in February 2018. These indicators for integrating cyber security of the new evolving energy industry. (see attached)

The principal of Alive Information, Robert Relf, is also a member of the Systems Engineers Society Australia, the IoTAA as well as NERA and the Joint Cyber Security Centre, Melbourne. Comments put forward are from colleagues comments for this Point of View towards Critical Infastructure

A more formal submission could be presented given more time, but this year, especially in Victoria, has not given enough time for more detail.

The focus is towards the Trusted Information Sharing Network (TISN) for Critical Infrastructure

In response the “Call for Views” the comments below have been added to the 36 Views items of the above paper.

Regards,

Robert Relf   Email: [redacted]

With Reference: **"Protecting Critical and Systems National Significance – Consultation Paper"**

Ref. Comment

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 needs national governance with international input at a DoD level.
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?**
	Industry input is required to establish floating tiered levels of risks. These risk levels having registered levels based on their consequential loss levels. This will need to include encrypted key registrations. *There seems to be confusion on the general understandings of cyber security and cyber risks. Particularly with respect to the Positive Security Obligations which need to be changed from "all" hazards to "known" hazards. Much of these issues have been established in the assessments of Major Hazard Facilities(MHF) but only governed at a state level.* *There is an opportunity for national register of MHF and their associated risk levels including the data generated from these facilities. This does need examination.* *In the Personal Security the promoting of a 'positive and collaborative security culture of continual improvement and engagement across sectors" needs to be built on a risk level not a security level. This so insured risks may be clearly defined.* *Privileged Access Management(PAM) design guidelines for best practice will also be needed.* *Considerable work for a national system appears to be needed.* *When well designed lateral integration will be able to be achieved.*
10	**Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?**
	The item "security risk" needs a clearer definition. *Similarly the "Supply chain security" has "understanding of supply chain risk"*
16. 21	**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?**

	It has been noted the short falls in Essential 8. The five point process monitor is a good start but applying in concepts across the 11 areas of Critical Infrastructure will need consulting. There are also international tools being developed beyond NIST, etc *The “Education Guidance” is a good topic but needs development by industry bodies, not TAFE or similar RTOs.* *The legal concepts need re-examination so all State and national regulations will have a common legally binding agreement. This will need to include the international regulations and the different foundations upon which they are presented.* *The Transport Certification Authority(TCA) has attempted a national system with basic success. An industry today cannot grow on arbitrary standards.* *A secure or hardened configuration is one that only allows ports and services required for operation, provides only necessary privileges, disables less secure protocols, disables unnecessary accounts and changes default accounts and credentials. Defined secure configurations are critical to configuration management and disaster recovery programs.* *This is a great export development opportunity.*
27	**What information would you like to see included in playbooks? Are there any barriers to codeveloping playbooks with Government?**
	The”Playbook” is a good concept (fig 4) and will be very much needed as the data management will explode with IoT and IIoT data input. This is currently in good development with the several working groups within the IoTAA. The IoTAA is outlined in the Telstra “Australia’s 2020 Cyber Security Strategy” submission. *As per “25” there will need to be new methods to establish and identify critical networks especially where a national approach will have far greater benefits than state only governance.*
29.	**In what extreme situations should Government be able to take direct action in the National Interest? What actions should be permissible?**
29, 35	*At all times. A framework designed for the national interest will be by far give the best solutions. Variations of templates levels and risks need to be designed to suit the environment and the particular locations.* *These are issues being addressed internationally and Australia needs to have continuity in frameworks so Australia may export best solutions as well as integrate with international best practices. e.g. NIST, CIS as well as international standards.* *This year there has been a release by the DoD, USA to set levels. They have created the Cyber Security Model Certification. This is being put forward this year by the Department of Defense , USA focused towards Procurement an acquisitions, which I will include services.*

	There has been a lot of work to put this together and I suggest you take some time and research this in greater detail. *Internationally, this has started with Five levels to pursue. Nearly all of us will currently be at Level 1, but it will be good for industry groups to start to have common goals.* *Being USA based it is focused on Federal Acquisitional Regulations then linking to the 48 practices of NIST. NIST is the National Industry Standards and Technology and has the National Cybersecurity Centre of Excellence.* *In Australia, while we can take initiatives from the USA, history has shown we do need to create the Australian versions for implementation.* *The critical status and tiered approach is most likely will be needed for Hospitals, medical equipment and elderly accommodation and condition monitoring.*
36	**Does this mix the 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 of Government.**
36	*The tiered system will clearly separate responsibilities but will need overall governance rather than has experienced by COAG agreements in the past.* *The legal status of the different tiered levels will need to be developed.* *These are international challenges and Australia will need an Australianised version of international standards.* *Aust Cyber is taking an excellent approach to give opportunities to develop Australian industries. However the IoT and IIot data link ups are multiplying the data resources by a factor of ten and will need orientation into the water and primary industries with national standards and integrated cyber risk levels.* *The splitting of the Murray Darling Basin Authority is a good start.*