CyberOps Protecting Critical Infrastructure

Consultation Response

CyberOps

www.cyberops.com.au

sales@cyberops.com.au

This page is deliberately blank

Introduction

CyberOps Pty Ltd is pleased to respond to the Consultation Paper released in August 2020 by the Critical Infrastructure Centre in the Department of Home Affairs.

CyberOps is an Adelaide-based company that specialises in the means to strengthen the cyber security of Small and Medium Enterprises (SME) that are seeking to enter the Defence market. The founders of CyberOps have extensive experience in Defence notably Defence research. They are well-versed in the security requirements of the Commonwealth that are outlined in the Protective Security Program Framework (PSPF) and the Information Security Manual (ISM), the specific requirements of Defence, expressed through the Defence Industrial Security Program (DISP) and relevant international standards as well. More information about CyberOps is here.

CyberOps has developed a cyber framework and security architecture, from which a process and service offering have been developed, that allows companies, Small and Medium Enterprises (SME) especially, to assess their 'Defence readiness' from a security point of view and to therefore understand, what they need to do to become 'Defence supply chain ready'. This is a low risk, inexpensive and practical assessment process. The tool has been demonstrated to more than 100 companies, including a number that are involved in the developing space industry sector of the economy. An outline of this process is here.

CyberOps is also developing technologies that enhance Australia's sovereign space domain awareness (SDA) capability.

These capabilities can be readily broadened to the critical infrastructure identified in the Consultation Paper.

Response

CyberOps has provided comments against each of the 21 Questions posed in the Consultation Paper drawing on the experience and background outlined above.

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 Consultation Paper, in its opening paragraphs, speaks to interdependence and interconnectedness, then identifies 11 sectors that stand somewhat in isolation from each other. There is point to this because of the importance of intra-sectoral communication. Farmers, for example, need to talk to farmers and bankers to bankers about specialised aspects of their businesses. However, the relationships that exist between the sectors are critically important to understand as well. There may be, for example, single points of vulnerability, if not failure in the storage and distribution network of a water supply system that:

- relies on a commercial telecommunications provider for the command and control of its distribution network, with no back up;
- assumes that power from the grid will be available to support water, release valves from dams and the pumps needed to move water around the network, i.e. there is no or minimal investment in uninterruptable power supply (UPS) systems at critical locations and nodes in the network; and
- stores data in the cloud (some, if not all, quite possibly offshore) with little or no appreciation of the risk and vulnerability that such data storage solutions present.

To draw an analogy, the weakest parts of any item of clothing are the seams. This is where tears occur when the garment is stressed. This principle is very much in evidence as Commonwealth, State and Territory Governments response to the COVID-19 pandemic. Failure has occurred (Ruby Princess, quarantine hotels, aged care, closed borders with unintended consequences on primary producers with farms in adjacent States, etc) where jurisdictions intersect. Planning and coordination mechanisms and clear lines of command and control, responsibility and accountability have been absent.

We would argue that, as a matter of urgency, and taking account of the all hazards approach that underpins the logic of the Commonwealth's approach to critical infrastructure resilience, that attention be paid to developing architectures that demonstrate unambiguously, the relationships and communications structures between the 11 sectors identified in the Consultation Paper, their mutual dependencies on each other and common supply chain providers. A single point of failure in one sector may seriously impact and even cripple another sector.

With specific reference to the sector defined as "Defence Industry", our view is that this is a misnomer and could mislead analysis and wise response. There are four points to make.

- In the past thirty years or so, many Australian manufacturing companies have closed because they have not been able to compete on price, and sometimes on quality, with similar goods imported from overseas. One consequence is that manufacturing in Australia has been hollowed out creating supply chain vulnerabilities now recognised by the Australian Government and recognised in the Consultation Paper. Heavy engineering and textiles, specialist electronics, clothing and footwear (TCF) are examples.
- Many of the manufacturing businesses that have survived serve niche aspects of the domestic market, a sub-set of which is the Defence market. Some companies may provide components well down in the supply chain that are important, even essential to a defence capability without having any knowledge of that dependence. These companies do not think of themselves as Defence companies and have no interest to become 'Defence ready'. Rather, this illustrates the dual use nature of many goods and services now used by Defence.
- To remain viable, numerous of these companies have developed export markets, mainly in the civil and not the Defence domain. Australian laws and international treaty and other obligations place significant limitations on the Defence equipment that can be exported and the countries to whom we might sell such goods and services. Civil markets, in contrast, are larger and more easily accessed.
- Very few Australian companies exist today that have the ability to design and manufacture the machines and the tools that are used to make components and assemble them into finished products. The domestic market is too small to sustain the high levels of investment needed to re-tool and re-equip Australian industry across the board. Whilst the Commonwealth may assist companies to re-tool and re-equip to meet the needs of Defence, the companies that benefit are but a subset of the national manufacturing base.

To summarise, we argue that a more helpful discussion about the current state of Australian manufacturing and the desired future state should explicitly recognise that Australian companies which explicitly support the Defence enterprise are regarded as a sub-set of Australian manufacturing industry overall. A broader approach, under a heading such as Manufacturing Industry, may lead to more resilient outcomes. This approach would view Defence industry as a sub-set of a much larger sector. It would also recognise the 'dual use' nature of many of the goods and production processes that are essential to advanced

manufacturing and that support most of the critical infrastructure sectors identified in the Consultation Paper.

A further point, and this is an important element of CyberOps' space related business, is that Australia must invest in knowing how to develop particular manufacturing capabilities if forced by international circumstances to do so. We need to understand designs and modern production techniques to develop an adaptable manufacturing sector that can be turned quickly to produce goods which would normally be imported or for which there is no usual demand. Examples of this is the rise of 3D printing, and the way in which several Australian companies adapted their factories to produce masks and ventilators in response to the COVID-19 pandemic.

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

The present definition of critical infrastructure (Consultation Paper, p11), would be strengthened if a temporal element were added or at least alluded to. Some disruptions may occur quickly and with little or no warning as a consequence of natural events (e.g. a massive solar storm or bushfires in catastrophic weather conditions) or of human activities (e.g. cyber or terrorist attack). Other disruptions may build over time (e.g. drought or failure of vital structures such as key bridges). Critical infrastructure systems need to be able to absorb significant unforeseen shocks as well as being able to cope with insidious, incremental threats.

Using different language, the current definition looks to the impact on society of the loss of critical infrastructure assets and capabilities. Perhaps there is merit in commenting on the attributes, business and technical, that should be designed into critical infrastructure systems to strengthen resilience leading, when attacks do occur, to graceful degradation rather than catastrophic failure.

The current definition speaks to physical and virtual systems with no reference to the vital role of people in critical systems. People and the experience and wisdom they possess are often the most difficult and long-lead time element to replace in any complex system. Similarly, broader industry impacts when key people are impacted by pervasive societal events, who are relied upon to support critical systems e.g. family members affected by COVID-19 impacting on critical emergency services and incident management capabilities.

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?

Extending the responses to Questions 1 and 2, and perhaps somewhat radically, consider redefining critical infrastructure as the relationships, dependencies and interdependencies that exist between nominated sectors rather than the sectors themselves.

We suggest that the advantages and risks of supply chain complexity and diversity be given prominence in the legislation and policies to come. To the extent that complexity allows for truly alternatives in supply of materials, production processes and distribution networks, a more resilient system emerges because it has more options by which to adapt when confronted with existential or even serious threat. This is certainly the case with regard to cyber risk.

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

As a SME working in the cyber and space domains, the threats to CyberOps' business continuity are:

- Unscheduled non-availability of key staff (due to illness, injury or other unforeseen events;
- Cyber attack; noting the high level of interest shown by malfeasant actors in Australia's current and developing capabilities in the cyber and space domains;
- Demand overload, when issues arise for one company, then they tend to be front of mind for others which leads to large demand spikes which are hard to manage for a large company, let alone a SME;
- The reactive response required to respond and recover from Cyber attacks within immature Australian business, results in resources need to be mobilise in very short timeframes to satisfy incident response needs. Concurrent events stretch available resources to respond in a timely manner, extending the impact of all events.
- Uneven cash flow, largely a function of the small size and immaturity of the markets in which CyberOps operates.

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

In order:

- Threats to life – immediate, then longer term
- Threats to livelihood – immediate, then longer term
- Threats to Australian territorial integrity
- Threats to Australia's value system and way of life
- Threats to critical services and dependant supply chain services.

These are neither mutually inclusive or exclusive and, as we have observed with the pandemic, balances need to be struck that are not universally agreed or accepted. Whilst the nation state exists as the fundamental institution of national and international order, priority should be accorded to the creation and maintenance of sovereign capability, that translates to self-sufficiency and resilience.

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

Water and energy sectors and core communications and transportation companies should certainly be operated by Australians and ideally have Australians owning controlling shareholdings as well – either through government or private enterprise arrangements. Why? When infrastructure is new and running well, the repatriation of profits to offshore owners, as happens today in the energy sector especially, is of no great concern – providing the foreign owners pay their fair share of tax. However, as we see today with baseload power in NSW and Victoria, the foreign companies that own these power stations are looking to shut them down early and to not re-invest.

This points to the fact that critical infrastructure policy is a sub-set of and dependent on higher level policies that are coherent and have broad community consensus including for climate change, energy and national security (of which Defence policy and capability and critical infrastructure policy are but sub-sets). There is evidence that Defence is purchasing more from domestic suppliers today than has been the case for quite some time. Perhaps critical infrastructure providers can be encouraged to do the same.

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

There are several elements to our answer to this question.

- The first element is to support the inclusion of "Data and the Cloud", "Education, research and innovation" and "Space" as sectors critical to Australia's economy and security.
- The second element, already mentioned, is to argue that the reforms to the TISN and to the CIRS may not achieve much improvement, unless coherent higher-level policies are developed, legislated and achieve broad community agreement or acceptance.
- The third element involves how the TISN and CIRS are communicated to Australian industry, especially to SMEs. These companies typically do not have the time and headspace to deal with the many complexities of Government bureaucracies – even those parts of Government that are designed to facilitate and assist business. The 'what', 'why' 'how' and 'when' questions that the proposed reforms raise will need to be answered in terms that are crystal clear, unambiguous and easy to grasp.
- The fourth element is to note that in our experience the value of the TISN faded away, to the point that its impact and influence was substantially reduced. Both Government and Industry need to commit to the TISN for the long haul and ensure that it really does encourage and support genuine information exchange that is valuable and that serves to ensure that Australia's critical infrastructure is more resilient and secure.

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

To this point, the TISN has mostly serviced large companies with staff who are devoted to security, risk, government relations and business intelligence. These companies continue to need to be serviced. The challenge is how to introduce the Positive Security Obligation (PSO) to SMEs, some of which provide critical goods and services to larger companies that are unique and for which there is no, or at best, limited supply chain diversity.

Many of these companies have no experience of, or interest in, security beyond the locks and alarms that protect their physical premises from unauthorised entry. Security is likely to be regarded as a cost to business, offering no positive advantages. Further, the present Government has a policy mantra to reduce red tape. The PSO runs counter to that commitment.

This reinforces the point, made in the response to Question 7, for well-resourced industry education/skills programs and materials that assist companies to assess their requirements and, where required, degree of compliance/non-compliance with Government directives, laws and regulations.

These materials might be most effectively disseminated to SMEs through existing peak bodies such as AiGroup and the Council for Small Business Associations (COSBOA), professional bodies, such as the Law Council and Engineers Australia and industry groups as well. Beyond generic information that might be disseminated via these means, tools and follow-up services such as those developed by CyberOps should be actively promoted – perhaps through a registered panel of pre-approved service providers.

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?

As noted in the answer to Question 8, through education, regular engagement and easy to access tools and aids. Case studies may be especially important as a means of persuading many companies that have never thought much about security at all, to highlight that they are part of a much larger critical infrastructure eco-system.

Any costs accrued by companies in achieving their PSO will be deductable as legitimate business expenses. This point is worth reinforcing as the changes to legislation are drafted and announcements about the proposed changes are made. Depending on the urgency with which Government seeks to achieve broad acceptance of and investment by companies in achieving the PSO level appropriate to them, Government may consider other financial inducements such as some form of rebate scheme certainly for elements of the PSO that a mandatory.

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

Yes. The addition of supply chain risk to the traditional three – physical, personnel and information - is especially welcomed.

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

Yes, but, the question, as discussed above, is how to make the PSO a part of the business of SMEs that enters the culture of small companies as a positive and valued dimension of the business rather than another cost and burden to be endured.

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?

Larger organisation with which we deal, many of which are Defence suppliers and members of the DISP have embraced the principles of the PSO as part and parcel of their normal business practices. A similar comment applies to smaller companies with which we deal and that also work with Defence. However, we know of a number of start-ups that are resistant to adopting even quite modest security standards on two bases – cost and the negative impact on innovation. We can also point to other companies, that having made a decision to improve their security posture and that have been pleased with the outcome as they are now more aware of their true exposure and their actions to reduce this risk.

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

There are direct and indirect costs. We assess the direct financial costs to be mainly incurred in better protected and managed computing and data management and storage systems and in the audit of those systems. The indirect costs will be in the time cost in learning about the PSO and implementing the security systems and processes that are needed. There is also an opportunity cost; time spent on PSO matters means less time being spent on moving new companies from a start-up basis to a solid footing basis.

The direct costs in dollar terms form small organisations are probably measured in the thousands for start-ups and maybe low tens of thousands of dollars for small companies.

These costs are annual and recurring. Part of the educational challenge for some companies is to have them understand that security systems and processes need to evolve in line with the evolution of threats and the broader threat environment on the one hand and the evolution and development of their business on the other.

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?

In our experience several of the sectors identified in the Consultation Paper, in general terms, behave in accord with the principles proposed to underpin the PSO. These include: Banking and finance, Communications, Data and the Cloud, Defence industry, Health, Space and some aspects of Transport and the national research institutions (CSIRO and DST Group).

We make the point once again, the level of understanding, acceptance and, where needed, compliance, with risk and security practices is less in smaller organisations than in larger organisations. There seems also, in our experience to be a correlation between the behaviour of companies that are publicly listed and those that are privately held. To generalise somewhat, the standard of governance of publicly listed companies is generally higher than that applies by privately held companies, especially those held by owners and founders.

We are aware of companies that had simply not considered the importance of risks to their business beyond the flow of orders and cash in the bank until they sought to become suppliers to Defence. In recent years the Centre for Defence Industry Capability, through its Business Advisory Program, has helped numerous metal fabrication companies from being dirty and disorganised to holding ISO certifications and being accredited suppliers to companies including Pratt & Whitney and Lockheed Martin.

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

The devil will be in the detail. It is imperative that any new regulations proposed are harmonised with existing regulations and relevant national and international standards. Examples of relevant national standards are the DISP, rules relating to the employment of foreign nationals in certain positions and the increasingly stringent cyber security regulations being imposed by some foreign governments and private entities headquartered outside Australia. An advantage of clearly articulated rules and standards across the sector is that the movement of skilled staff within the sector should be facilitated, adding resilience and strength to the sector as a whole.

Companies must be able to understand their regulatory obligations quickly and unambiguously and to be able to seek advice and reassurance from people when uncertainty still exists. The Defence Security Authority struggles to fulfil its obligations under Australian law and to our allies as well. Home Affairs should not under-estimate the magnitude of the task on which it is embarking through strengthening Australia's critical infrastructure protection regime, especially with the addition of the need to protect supply chain.

The assessment tool developed by CyberOps, with appropriate modification and continuous review and update, would provide one method by which companies and other entities can access current information about threats and their PCO obligations in response.

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?

Our comment is not so much about content as it about presentation. The guidance MUST be written from the point of view of the reader to have any chance of wide uptake and acceptance. Plain English (and possibly other languages as well) and convincing rationale will be essential. Case studies relevant to particular sectors and sizes of business are one method of making the threat real and therefore the rationale for investing in security, equally convincing.

Whilst Government must abide by diplomatic protocols, meaning that some State actors that are culprits may not be named, the types of attacks and the damage caused needs to be spoken about as openly and frankly as possible. This will assist Australian companies to undertake timely risk assessments on their own organisations in relation to the disclosed threat.

Security, especially of people and information, is not intuitive to many people and runs counter to the values of liberal democracy. The broader communications envisaged must take such matters into account , be sufficiently articulated and convincingly explained that public criticism of the scheme can be readily and effectively countered.

Different countries have adopted different tones or voices in how they state their protective security requirements. One example is the contrast between New Zealand's *Protective Security Requirements* and the *Australian Protective Security Framework*. The former is in plain English and written from the point of view of security as an enabler to business. The latter emphasises compliance and the potential costs of non-compliance. Australia would do well to take a leaf from New Zealand's book when making revisions and additions to our national protective security framework.

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?

We think the case is developing for a national protective security organisation that subsumes the Defence Industrial Security Program (DISP) and the Australian Government Security Vetting Agency (AGSVA). These functions have defaulted to Defence in the absence of a compelling need from any other sector of Government, except the intelligence community, to invest in such capabilities. They incur a substantial cost, especially in people – those who conduct the security clearance assessments of people and who accredit the spaces and information systems of organisations beyond the Commonwealth that handle classified material.

Possibly more important than who should do the work, is the imperative to ensure that the certification, approvals, oversight and review process in place is appropriately funded and resourced. Today, security clearances, especially for people working in industry can take many months and, in the case of the highest level clearances, years to obtain. This situation is not defensible and runs counter to the Government's desire to make the nation's critical infrastructure more resilient. In our experience, industry does not mind paying for clearances, but there is an obligation for the process to be conducted in reasonable time and, for the Commonwealth to keep vettees informed of progress, especially where delays are encountered.

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

Above all, the sector regulators need to know who to call for authoritative advice and rapid response. The regulators also need to be confident that their calls will be answered by people who are appropriately trained, authorised to provide the sought after advice and that they will respect commercial and other confidences.

Advice needs to be provided in a way that is understood by technical and non-technical individuals i.e. use of plain English, real world advice and positioned in an industry segment context. In this regard, and as noted above, we recommend an approach be taken the emulates that taken by New Zealand in its *Defence Security Requirements* documentation.

A common approach across sectors that nevertheless acknowledges different standards and controls that are sector specific is strongly encouraged because of the many cross-dependencies that exist between the identified critical infrastructure sectors.

Finally the Australian model or approach should map to the requirements of our key global trading partners – pointing out where there is and is not equivalence and making clear that where an Australian organisation meets a more stringent international standard, by default it will be deemed to have met the Australian standard as well.

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

By being continuously more open, more engaged and more timely in alerting sectors to specific threats and by more carefully and in non-alarmist, ideological, racist or similar terms. Inform the broader public of the type and extent of malfeasant activities, which are now more or less continuous and increasingly difficult to counter. There is, of course a cost and the challenge for Government is to balance the cost of responding adequately to the threats that are mounting, seemingly on a daily basis against all sectors of Australian society and the Australian economy.

By providing a high-level security architecture that is tailored to the sector, that not only looks at the individual organisation, but also the wider ecosystem and its dependant relationships with other supply chain capabilities (possibly across industries). This encourages common terminology and high-level approaches for organisations to compare their approach to and to better assess pervasive risks.

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?

In a word, with difficulty, unless the argument is carefully and patiently made in the broader community. The charge from some sectors of the community is that Australia is becoming a "police state" or a "surveillance state". The argument needs to be linked to the values of liberal democracy, a fair go and to the safety and security of jobs and our countries interests.

We need to be careful not to over-clear people to keep costs and time delays within reasonable bounds. We also need to acknowledge that vetting agencies are not funded or staffed to deal with mass increase in number. Conversely, at present the AusCheck scheme is a point in time check with little or no capacity for follow-up or on-going checks. Any

enhanced personnel security program that emerges from Positive Security Obligation needs to have national application and work across all critical infrastructure sectors to permit individuals to move seamlessly between the sectors without the need to establish their credentials or bona-fides from scratch.

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

CyberOps has recently completed a Defence project to deliver a Cyber Framework for the Space Industry that addresses the needs raised as part of the Critical Infrastructure review. We encourage further discussion on how we get this process widely adopted. The framework is in alignment with the approach taken by other Australian sectors that also fall under the same review.

We would like to see increased emphasis on identifying and ensuring cyber resilience is established for critical economic and societal reliant services is required not just for Systems of National Significance (SONS) but more broadly. We would also like to see some guidance as to the expectations and responsibilities of the providers of cyber security services

Current emphasis is to strengthen the cyber security of the SONS. This makes sense as a place to start but overlooks a number of complexities. Some SONS will have dependencies on organisations that are defined as being in the second or lower tiers in terms of their criticality. It is also possible to envisage situations where two or more second level services could fail, creating the same or more dislocation that the failure of just one SONS. This points to the urgent need for comprehensive supply chain and dependency mapping of all critical infrastructure supply chains, potentially reaching down to component level providers.

Most modern government policies support the need for industry driven policies and programs. In the case of critical infrastructure, if we are serious about strengthening national resilience, Government must establish adequately funded and resourced oversight mechanisms to ensure the rigour of these activities, avoidance of duplication, or overlap, and to provide mediation for different industry views where necessary. An important challenge for Government will be to develop metrics against which resilience can be measured and that make sense to the critical infrastructure sectors themselves and to the broader community as well.

There follows a series of points, some of which have been touched on in general terms in responses to previous questions. Here the points relate specifically to the cyber security dimension of strengthening Australia's critical infrastructure.

- A wholistic approach to Cyber across the critical infrastructure and industry supply chain offers the possibility for greater positive impact on Australia's business and society than does a piecemeal approach.
- Although industry should lead, in the sense that it accepts principal responsibility for its own security, the essential role of Government is to create the environment and the opportunities for consultation, coordination and collaboration in and between all critical infrastructure sectors and beyond , leading to cultural change and to wide acceptance that security, in all its forms, is a plus for business and not a cost to be endured.
- Transparency will be vital. Governments must provide the "why" behind decisions, in order to build trust between government and business and the broader community.

- As critical infrastructure policy and procedures are developed, Governments must accept that many businesses in critical infrastructure supply chains, notably the SMEs, lack the people, time and money to put in place all but basic security measures. This reality reinforces the point for clear and unambiguous direction, especially with respect to mandatory requirements and for using existing relevant industry standards and certifications wherever possible.
- Identify opportunities to implement partial or easy to understand cyber maturity indicators.
- Increase opportunities or reduce barriers for business and society, to undertake greater cyber resilience cultures and steps.
- Establish longer term and bi-partisan consensus that build enduring cyber security positions and strategies. One aim is to provide business and society a set of common goals that would reduce anxiety and uncertainty over time.
- Companies that supply goods and services to Australia's critical infrastructure sectors, whether locally or from overseas, should be required to provide a minimal level of security.
- Existing industry standards, where they exist, should be used as the basis from which to develop more exacting guidance that, once followed, will add to the critical infrastructure resilience sought by government.
- A Cyber health indicator system, similar to the food health or energy star system, might be one relatively simple way of informing the community about the importance of cyber security and the degree to which a particular organisation is cyber resilient. Such a public rating would reward suppliers for the efforts they take to become cyber secure, and would enable them to inform customers that they take security seriously.
- The cyber star system proposed in the previous point would need to be introduced gradually and supported by industry. This should not be too onerous for new services where the star ranking might consider for example, the assessed cyber resilience of the organisation in terms of its dependencies/interdependencies, an industry/user impact risk assessment and whether or not the organisation supports any critical service delivery process.
- The Australian Cyber Collaboration Centre (AC3) in South Australia may contribute to establishing baseline requirements and testing in conjunction with other research institutions, businesses and academia.
- This may in part be a peer business or industry driven metric, to ensure supply chain and interdependencies are considered.
- Establish a system of testing/certification – something that A3C, and similar organisations could assist in doing on behalf of the government.
- Establish a level of testing similar to the certification of electrical installations, relating to the cyber quality of products used by critical infrastructure providers.
- Establish sovereign and trusted threat/support networks that are available to industries and the Australian public.