AustCyber
Australian Cyber Security Growth Network

SUBMISSION

PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE

DEPARTMENT OF HOME AFFAIRS
CRITICAL INFRASTRUCTURE CENTRE

SEPTEMBER 2020

Digital risk to digital trust

AustCyber welcomes the opportunity to respond to the Department of Home Affairs' (DHA) Critical Infrastructure Centre consultations outlined in the *'Protecting Critical Infrastructure and Systems of National Significance Consultation Paper August 2020'* (Consultation Paper).

These consultations are timely. Australia has critical dependencies in the digital domain and therefore on the trust and security of all digital activity. With accelerated uptake of digital technologies in response to the COVID-19 pandemic and more day-to-day activities moving online, the data presented and its analysis is an important contribution to the reframing of the nation's approach. Focus is needed on ensuring the digital environment is secure, resilient and effective.

Australia's Digital Trust Report 2020 (Digital Trust Report) published by AustCyber in July 2020, argues that key sections of Australia's economy are undergoing a step-change because of rapid transition to a more sophisticated, interconnected digital environment. The Report found that digital activity currently contributes AU$426 billion to the Australian economy and generates AU$1 trillion in gross economic output, generating one in six jobs.

To underline the importance of digital trust, the Digital Trust Report modelled the economic impact of a four-week digital interruption to Australia's economy, such as through a widespread cyber attack, would cost the Australian economy AU$30 billion, or 1.5 per cent of Australia's Gross Domestic Product. This is estimated to be equivalent to losing over 163,000 jobs. The economy-wide need for cyber security and resilience is what makes the cyber security sector Australia's true horizontal enabler.

To build and secure digital trust, Australia must continue to invest in the means to secure digital infrastructure and data to not only assure trust but to also sustain efforts to reboot growth. The Digital Trust Report measured the direct value of cyber security as generating nearly $16 billion in revenue and 19,000 jobs and AustCyber's Sector Competitiveness Plan estimated that Australia's revenue from cyber security could triple over the next decade.[1]

With the cross sector focus on digital trust through embedding protective, robust and resilient cyber security across all digital infrastructure and the wide-ranging approach outlined in the Consultation Paper, AustCyber has taken a cross-sector and industry approach to examining the changes and issues of proposed by DHA.

[1] 2019 Update to Australia's Cyber Security Sector Competitiveness Plan, AustCyber, https://www.austcyber.com/resources/sector-competitiveness-plan

Industry views

In developing the positions in this submission, AustCyber has consulted with a wide range of industry stakeholders across large and small organisations in a variety of sectors about the proposed amendments to the *Security and Critical Infrastructure 2018* (SOCI Act) outlined in the Consultation Paper. They include organisations delivering technology, networks and infrastructure; delivering cyber security products and services; and organisations that acquire and use cyber security technologies and capability to protect and keep information and digital systems secure and resilient.

From these discussions, which have taken place since the Consultion Paper was released, there is a general view the critical infrastructure regulatory arrangements need strengthening and expanding to ensure a heightened industry security posture. Ensuring there is consistency in the approach adopted across industry, sectors and organisations within Australia is welcomed. As has been the experience of the NSW Government's Cyber Security Standards Harmonisation Taskforce, which AustCyber co-Chairs with Standards Australia and the NSW Minister for Customer Service, it is anticipated there will be instances where industries can enhance their security approaches in ways that are likely to be relevant to and can be shared across other industries and sectors.

Further, there is also merit in the Australian Government designing arrangements that are consistent as much as possible with what other countries are doing. Australian industries, including soveriegn cyber security companies, increasingly aspire to and take advantage of global opportunities in markets outside Australia. Operating in an onshore environment that is consistent with regulatory approaches offshore provides a foundation for companies' products and services to be exported into other markets efficiently (the economic persepective) and more effectively (the security perspective). This is particularly the case when operating across Five Eyes countries.

All stakeholders engaged recognised that industry has been improving its security posture in response to the changing threat environment and it is continually working to improve these arrangements. However, various technology and information system providers are at different levels of maturity than others.

AustCyber can see the potential for the framework as described to create opportunities for organisations, industries and sectors to collaborate on developing best practice protections and responses to threats, as well as to also share what they are learning resulting in greater consistency across industry more broadly and a drive for continual improvement.

AustCyber welcomes the approach recommended by DHA becoming a platform for collaboration, not only in working through the standards and regulations to apply under the amended SOCI Act, but more broadly as industry participants share their experiences and integrate not only their networks, but also their successful approaches for building cyber protection, threat response and resilience.

Different obligations on critical infrastructure providers

There is support for different obligations on different categories of critical infrastructure, so that 'systems of national significance' face the more detailed 'Enhanced Cyber Security Obligations' (ESO) and other critical infrastructure are subject to the relatively 'lighter touch' requirement to meet the principled 'Positive Security Obligations' (PSO).

Critical infrastructure entities

The Consultation Paper asks whether the current definition of critical infrastructure is fit for purpose. It notes that the Australian Government's Critical Infrastructure Strategy currently defines critical infrastructure broadly, and with critical infrastructure to encompass a wider range of infrastructure, and a larger number of entities, AustCyber can see merit in this definition continuing:

> '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 social or economic wellbeing of the nation, or effect Australia's ability to conduct national defence and ensure national security.'[2]

Critical infrastructure entities are to be those in designated critical infrastructure sectors and are to be subject to PSO which are a set of principles-based outcomes to protect entities from all hazards, which could include natural and human induced hazards. These PSOs include having plans in place if a natural disaster, pandemic, cyber security incident was to take place. As many organisations would have plans to cover such incidents currently it will be important that PSOs do not create duplication and existing plans are recognised with opportunities for improvement.

We also see significant merit in opening discussions with industry over time, following the initial implementation of the proposed reforms, on evolving the definition to focus on **critical services** and the role critical technologies play in support of their delivery. Other nations, including some of the Five Eyes nations, have moved in this direction which acknowledges the increasingly horizontal nature of digital infrastructures and the hyper interconnectivity of these infrastructures, and the data they carry, across sectors and within sectoral segments.

Moving in this direction also supports the increasing harmonization of standards and guidance occurring at the international level, which in turn supports industry to sustain and innovate on its competitiveness and comparative trade advantages as well as Australian governments to develop and enhance common lexicons and terms of knowledge exchange, especially important in times of crisis that cross jurisdictional borders.

Roles of the regulators

DHA has indicated that in an effort to avoid or minimise duplicating existing regulatory arrangements, regulators that implement current industry regulatory arrangements for critical infrastructure entities, whether at the federal or state level, will be called on to supervise emerging threat environments. They will oversee the arrangements for PSOs.

The feedback from industry through AustCyber's consultations is that regulators have a range of expertise to be able to execute on these responsibilities and authorities, with some more experienced than others.

The Government will need to support these regulators so they are in the best position to support critical infrastructure entities to develop PSOs that draw on current best practice to minimise risks. This includes at the operational level, as well as strategic level, to account for different entities having different obligations under the Corporations Act and other concurrent legislation dealing with entity type and structure.

[2] https://cicentre.gov.au/document/P50S021, page 3

Systems of national significance entities

The Consultation Paper states that systems of national significance will include entities of the highest criticality. Given electricity, gas, communications, transport and banking have been considered essential services and the more important 'critical infrastructure', it seems reasonable for these entities to be moved into this 'highest criticality' category, notwithstanding the point above on critical services.

Systems of national significance are also to be subject to ESOs '…to help protect Australia's most critical entities prepare for cyber-attacks'. This is to include building '…active partnerships based on near-real time information to better understand and address threats'[3]. Building on the 2020 Cyber Security Strategy's action for enhanced cyber threat sharing, for the ESOs to function effectively, industry is necessarily seeking appropriate bi-directional threat sharing and more transparent dialogue on the resulting risks – which are highly contextual to industry segments and sectors; for some areas of cyber risk, the context is highly individualistic. Government and regulators being open to developing a deeper appreciation of this will help foster trust in bi-directional exchanges.

The development of playbooks

To support systems of national significance proportionately respond when facing a cyber-attack, DHA has suggested the Government and industry develop 'playbooks' to provide important information on 'what to do' and 'who to call'. This initiative is welcomed by industry and comments referenced the success of co-developed playbooks in the Defence environment. Reinforcing the views of industry, developing playbooks will need to be in a partnership between Government and industry with ongoing monitoring of their effectiveness also a collaborative effort.

Government assistance and direct action

The Consultation Paper indicates that entities may face situations where there is "…an imminent cyber threat or incident that could significantly impact Australia's economy, security or sovereignty, and the treat is within their capacity to address." The Consultation Paper also indicates there may be circumstances of an immediate and serious cyber threat to Australia's economy, security or sovereignty, including threat to life and the Government may need to declare a national emergency and instigate a national alert.

It is also explained in the Consultation Paper that taking direct action will depend on the entity's behaviour in response to a threat, so if they are deliberately non-compliant they are more likely to face penalties and or intervention by Government.

AustCyber considers that for clarity, transparency and to ensure the arrangements operate effectively, it will need to be clear the circumstances in which Government is to issue directions and to take the more intrusive direct action. Having a clear understanding of proportionality against entity size, age, relative cyber maturity and operating context – which perhaps need to develop for all parties over time – will also be important. The interaction of a direction with other potentially impacted legislation, such as the Privacy Act and concurrent state-based privacy frameworks, is another point of focus.

[3] https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf page 25

It is anticipated that through the PSOs and ESOs and encouraging a culture of collaboration and cooperation across critical infrastructure entities through commercially neutral incentives, these new arrangements will improve cyber security arrangements in critical infrastructure. If these arrangements are well designed and truly collaborative and combined with well designed, implemented and understood playbooks which make clear the emergency protections to be instigated, the need to resort to government direction or other forms of direct action should be a last resort and specified as such in changes to the SOCI Act.

With threat sharing an important foundation for entities to have the right information at the right time to ensure they respond suitably, the sharing arrangements developed in partnership with systems of national significance will be vitally important. They need to be developed in a way that makes sure there is an environment of trust and responsibility.

It is positive to see in the Consultation Paper that threat sharing requirements will be voluntary initially for less mature organisations, and over time it will become more of a requirement, enabling the Government and entities to become more expert in sharing threat information. However, in the meantime, the Government and the entities will need to create arrangements that cater for emergencies to ensure in a heightened threat environment, information is shared in real time and the information is meaningful. With access to the right sort of information that an entity can respond to, it will be able to respond quickly, taking the necessary protective measures.

Developing standards and other regulatory changes

DHA has indicated that after the SCOI Act amendments have been passed by the Australian Parliament, it will work with industry to design sector-specific standards. As discussed in Standards Australia's submission to this process, cyber security has a wide range of standards and regulatory requirements that are currently in place. Industry would like to see these standards and regulatory arrangements recognised and the co-design process commencing with the standards and regulatory arrangements mapped out.

The work of the previously mentioned NSW Cyber Security Standards Harmonisation Taskforce is to both map out these standards across various industries and develop a framework for harmonising and improving consistency as well as to work towards providing guidance to industry about how they are to operate most effectively. To minimise duplication and fast track this exercise, building on this work will be the best starting point.

The introduction of PSOs and ESOs across a wider range of infrastructure, networks and technology providers will require organisations to make sure they have the right security compliance skills and expertise available. With the industry facing a significant skills gap in cyber security, the ability for industry to meet the new regulatory arrangements in the short to medium term is likely to be hampered in some ways.

Delivering these changes will need skills and expertise

While discussing the expansion of the arrangements under the SOCI Act, industry explained to AustCyber that it will need access to further skills and expertise to meet the new obligations and requirements. The 2019 Update to AustCyber's Sector Competitiveness Plan estimated that around 17,000 more cyber security workers will be needed by 2026[4]. Work underway for the 2020 Update is already revealing a widening gap due to increased demand for cyber security products and services created by the COVID-19 pandemic – taking into account these new requirements, the need for skills is highly likely to further grow.

[4] https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3

TAFEs and universities around the country have rapidly expanded their cyber security programs in recent years, often in close partnership with industry. Approximately half of all universities in Australia are now offering cyber security as a specific degree or as a major in IT or computer science undergraduate qualifications. Another quarter offer at least some cyber security course units as part of various undergraduate degrees. Only 20 per cent of Australian universities do not yet offer any cyber security units or courses. This has led total enrolments and completions in university courses classified as security science to almost double between 2012 and 2016. Further, all TAFEs offering the TAFECyber program of nationally consistent, industry co-designed qualifications (also mapped to the US National Initiative for Cybersecurity Education's (NICE) Workforce Framework, below refers) are fully subscribed.

While this pipeline of developing the right skills and expertise is necessary, it is not sufficient.

To implement the changes necessary to address the growing skills gap, there also needs to be a focus on developing skills and professional expertise at higher levels which can come from a combination of additional professional training as well as on-the-job experience (including through internships and the like). Further, the arrangements being foreshadowed through the changes to the SOCI Act will also need highly experienced personnel that have deep expertise in dealing with and responding to intense threat environments.

The requirements for an increasingly diverse range of cyber security specialists has become more apparent. It is no longer useful to think of the cyber security occupation as one uniform job role or skill set. Today, cyber security comprises a range of technical roles from architecture to operations and newer, multidisciplinary, non-technical roles that incorporate elements of law, risk, communications and psychology.

While the face of the cyber security workforce is changing fast, Australia has not yet nationally endorsed a widely accepted skills framework to describe the various cyber security work roles. Other countries have, however, already taken action. For example, NICE has developed a Workforce Framework to standardise the taxonomy of cyber security occupations. It is a comprehensive, skills-based categorisation of cyber security roles. Companies in the US and other countries are using the framework as a common nomenclature for identifying the skills required in the cyber security workforce.

Recognising the need to grow cyber security skills to address the skills shortage quickly, AustCyber has adopted a national skills framework based on the NICE Workforce Framework[5]. The objective is to help build a common understanding between industry and education about skills needs and curriculum relevance, and to map a course curricula to align with this framework.

Over the last three years, AustCyber has been engaging with education and training institutions in Australia, alongside industry, to ensure that relevant work integrated learning has been built into cyber security curricula and that it is both regularly revised and the course structure accurately reflects current employer requirements.

While these activities are still gaining traction, AustCyber has already achieved a number of key outcomes. The NICE Framework has been leveraged and embedded across a number of education and training institutions across Australia. Several exemplars include the Canberra Institute of Technology, South Metro TAFE Western Australia, Queensland TAFE and Box Hill TAFE and New South Wales in vocational education. Leading universities adopting NICE include, the University of New South Wales, University of Queensland, RMIT University and The Australian National University. The number and pace at which additional institutions are incorporating the NICE framework is expanding.

[5] Part of AustCyber's role as a federally funded Industry Growth Centre is to provide workforce development to sustain growth in Australia's cyber security sector. For more information, see https://www.austcyber.com/educate

This is further demonstrated through AustCyber's Project Fund, which has funded five projects of national significance supporting cyber skilling and workforce development[6]. These projects also complement work under the Academic Centres of Cyber Security Excellence, funded under the Government's 2016 Cyber Security Strategy, the Digital Skills Organisation Pilot under the Department of Education, Skills and Employment, the National Skills Commission and cyber security skills mapping under the National Meeting of Digital Economy and Technology Ministers.

Interaction of the changes with the Telecommunications Sector Security Reforms

It is not yet clear what changes will be necessary for the Telecommunications Sector Security framework, also known as Telecommunications Sector Security Reforms framework, as a result of the proposed changes to the SOCI Act. Industry is keen to understand the impacts and welcomes further detail from Government on this.

Exposure draft of the amendements to the SOCI Act

DHA's industry consultations have indicated the intention is for the Government to introduce amendments to the SOCI Act to commence implementing these arrangements between September and the end of 2020. AustCyber and industry acknowledge these changes are needed, however they are significant, and we collectively request that an exposure draft of the Bill is provided to industry for further feedback. This will help to support the changes to be effective and provide information to the Australian Parliament on the ability of the changes to be implemented.

[6] Details at https://www.austcyber.com/grow/projects-fund

About AustCyber

AustCyber is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia’s cyber security sector, to support the development of a vibrant and globally competitive Australian cyber security sector. In doing so, our activities enhance Australia’s future economic growth in a digitally enabled global economy and improve the sovereign cyber capabilities available to protect our nation’s economy and community.

We form a part of:

- the Australian Government’s Industry Growth Centres Initiative, established through the 2015 National Innovation and Science Agenda, in sectors of competitive strength and strategic priority to boost innovation and science in Australia. Industry Growth Centres are required under contract with the Government to achieve for their sector:
  - increased R&D coordination and collaboration leading to improved commercialisation outcomes
  - improved management and workforce skills of businesses
  - more businesses, including small and medium enterprises, integrated into global supply chains leading to increased export income
  - a reduction in the cost of business through regulatory reform
  - additional or indirect (spillover) outcomes;

- Australia’s 2016 Cyber Security Strategy. It was through the industry consultation and development of this strategy that the concept for AustCyber was first conceived.

Our funding comes from majority Federal Government grants – funding for operations and programs, and for the AU$15 million AustCyber Projects Fund which provides grants to projects that deliver national benefit. We also receive funding under contracts with the governments of the ACT, NSW, QLD, SA, TAS, WA and the Sunshine Coast Regional Council and Townsville City Council, which we match, to deliver AustCyber’s national network of Cyber Security Innovation Nodes – with the NT and VIC soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into market ‘hot spots’ around the world.