Submission to the Australian Cyber Security Centre (ACSC) – *Protecting Critical Infrastructure and Systems of National Significance*

Submission from Standards Australia Limited – SEPTEMBER 2020

Standards Australia Limited ABN 85 087 326 690
Exchange Centre, Level 10, 20 Bridge Street, Sydney NSW 2000
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

16 September 2020

Mr Hamish Hansford
First Assistant Secretary
Australian Cyber Security Centre (ACSC)
Department of Home Affairs
CANBERRA, ACT

Lodged online

Dear Mr Hansford,

Thank you for the opportunity to make this submission to the Discussion Paper on *Protecting Critical Infrastructure and Systems of National Significance.*

For this submission, we have limited our comments to our expertise as Australia's national standards body, but we discuss specific proposals in the Discussion Paper.

For any questions or further information on matters raised in this submission, please contact Dr Jed Horner, Strategic Advocacy Manager, at [redacted] or via phone at [redacted].

Yours sincerely,

[redacted]

Daniel Chidgey
Head of Stakeholder Engagement

Table of Contents

Questions 1 - 3

> *We consider it essential that the cost of any regulatory reforms be considered with cross-functional dependencies. Traditionally, industry standards, some of which have involved certification, have played a constructive role here.*

The initial list of sectors in the Discussion Paper captures many areas that are either vital *or* important for Australia's national security and economic wellbeing.

However, some areas, such as cloud, are more overarching or horizontal. Others, such as food and groceries, could better be described as impacted in the event of risks materialising, but not necessarily with the corresponding magnitude or degree of risk to Australia's national security, including economic functioning. Having cross-functional dependencies highlights the importance of an approach centred on comprehensive risk identification, assessment and management in safeguarding critical infrastructure.

Below we address two specific issues for consideration in further developing these proposals, and which address questions 1 -3.

The interdependencies of sectors and the need for a proportionate regulatory response

It is conceivable that specific risks might materialise in sectors which are the result of nodal vulnerabilities elsewhere. For example, food and groceries might be impacted by payment system outages as a result of targeted cyber-attacks. However, the financial services sector is already a heavily regulated sector, with demonstrated resilience, granular cybersecurity approaches in place, and supporting industry standards, some of which are leveraged through the supply chain to improve cybersecurity posture.[1] For this reason, any proposed reforms should explore the extent to which sectors are 'responsible', in a regulatory sense, for broader impacts.

We consider it essential that the cost of any regulatory reforms is considered in light of these cross-functional dependencies. Traditionally, industry standards, some of which have involved certification, have played a constructive role here. They have enabled legal and, sometimes corresponding regulatory, obligations to be managed autonomously and in a streamlined manner through supply chains. More support for these approaches would be welcomed, particularly market support mechanisms for companies who are not as large and with a diminished capability to absorb the costs of any proposed regulatory reforms.

Using a sectoral approach to inform more targeted support, and intervene smartly

We note the cascading approach to defining, determining and classifying risks to national security and economic wellbeing adopted elsewhere, where sectors identified as of 'national significance' are used to identify specific companies, organisations and entities of national significance warranting further assistance or support.

This might include major infrastructure operators, scientific research organisations, law enforcement agencies and others. For example, New Zealand determines a classified list of organisations of national significance, as a basis for receiving advanced threat detection capabilities from the Government Communications Security Bureau (GCSB), with targeted

[1] In relation to this sector, an example is APRA's CPS 234, as well as baseline Management System Standards such as AS ISO/IEC 27001.

funding provided by the New Zealand Government for this purpose.[2] This also enables real-time reporting in relation to specific cyber security risks, as foreshadowed in the Discussion Paper.

[2] Government Communications Security Bureau (2020). *2019 Annual Report*. Wellington: New Zealand Government, p. 21

Question 19: How can Government better support critical infrastructure in managing their security risks?

We urge the ACSC, and the Australian Government more broadly, to be cognisant of the useful role that International Standards, developed by recognised Standards Development Organisations (SDOs), can play in this area.

Any measures adopted by Government, particularly those that seek to give effect to, or extend, the proposed Positive Security Obligation, should have regard to our trade obligations, in light of any security imperatives. Australia, and many of our trading partners, have obligations under the World Trade Organisation Technical Barriers to Trade Agreement to avoid creating Technical Barriers to Trade (TBT). As the WTO has noted:

> *Technical regulations and standards are important, but they vary from country to country. Having too many different standards makes life difficult for producers and exporters. If the standards are set arbitrarily, they could be used as an excuse for protectionism.*[3]

As a result, States are encouraged to use International Standards (developed by Standards Development Organisations such as the ISO and IEC), as a basis for any technical regulations or conformity assessment procedures they develop or adopt. There are other reasons for doing so, including the fact that where Australian expertise has been central to the creation of International Standards in the first instance, from a public policy perspective, this input can, and should, be leveraged back home. For example, the ISO Risk Management Standard (AS ISO 31000), used across sectors, arose from work in Australia and New Zealand, at least initially.[4] Additionally, Australians have undertaken significant work to develop Handbooks in these areas, adapted to the Australian context.

We note that many of the sectors listed in the Discussion Paper already have Standards relating to them, spanning risk management, security and resilience, information security, privacy information management and protective security, for example. These operate at differing degrees of granularity, and some provide broader guidance, whilst others can be certified to more formally. Some of these include:

- *Risk Management (AS ISO 31000)*
- *Security and Resilience (including ISO 22301:2019 – Security and resilience — Business continuity management systems — Requirements- as well as baseline Standards, such as ISO 22300:2018 – Security and Resilience – Vocabulary)*
- *Supply Chain Security Management (ISO 28001)*
- *Information Security (AS ISO/IEC 27001, and the broader ISO/IEC 27000 series)*
- *Privacy Information Management (ISO/IEC 27701)* – which is aligned with the EU General Data Protection Regulations (GDPR) and is currently being scoped for adoption in Australia, aligned with local legal privacy requirements.[5]

---

[3] See: WTO (2020). 'Standards and Safety', accessed 07/09/2020 from: https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm4_e.htm#TRS

[4] For a detailed case study, see: Standards Australia (2020). *An Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard*. Sydney: Standards Australia, Ref AI Roadmap case study, pp. 35-36.

[5] For a more detailed case study, see: Standards Australia (2020). *An Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard*. Sydney: Standards Australia, p.28.

In addition to the above Standards, there are obligations to align conformance assessment (which loosely refers to how accreditation and certification is designed, structured and undertaken), for any new proposed scheme or government approach. This is outlined in AS ISO 17021 (*Conformity assessment — Requirements for bodies providing audit and certification of management systems*). For example, ISO 17021 is likely to be referenced and leveraged by the United States Department of Defence, in embedding their new Cybersecurity Maturity Model Certification (CMMC) approach for the Defence Industrial Base.[6] This is because it reflects accepted good practice in conformance assessment globally, and there would be few reasons for a substantive departure from this approach.

We urge the ACSC, and the Australian Government more broadly, to be cognisant of the useful role that International Standards, developed by recognised Standards Development Organisations (SDOs), can play in this area.

We welcome further discussion to explore how Standards might be practically leveraged as ACSC proceeds with its important work in relation to both critical infrastructure protection and regulation and guidance material central to improving Australia's cybersecurity posture more broadly.

[6] CMMC Accreditation Body (2020). 'CMMC Third-Party Assessor Organization,' accessed 07/09/2020 from: https://www.cmmcab.org/c3pao-lp

Question 23: What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

> *In the interests of constructive public policy, we are of the view that the ACSC and other areas of the national security system might be able to leverage insights from partner agencies who already provide such functions in real-time or near real-time.*

The Discussion Paper proposes the creation of a process whereby Government would intervene, at a network level, in collaboration or in a 'declared emergency' in instances of identified, or likely, cyber intrusions. We defer to industry stakeholders on the desirability of this approach but do acknowledge that variations of this approach exist in other jurisdictions.

We are mindful that ACSC is likely already consulting partner agencies. In the interests of constructive public policy, we suggest that there is an opportunity to leverage insights from partner agencies who already provide such functions in real-time. For example, the New Zealand Government, through the Government Communication Security Bureau (GCSB) and the *CORTEX* program, provides malware threat detection and support to listed entities of *national significance*.[7]

This includes critical infrastructure providers and, reportedly, companies with a significant economic footprint, who are central to the nation's economic interests. We suggest that there might be scope to engage in identifying, with the agreement of the GCSB, how this reporting and integration practically takes place.

This might also provide the ACSC with insights as to how to manage existing legal requirements that might apply, including as they impact areas such as privacy. In the instance of particular deployments in New Zealand, privacy impact assessments have also been undertaken, subject to the appropriate classification of such documents at the time.

[7] Government Communications Security Bureau (2020). *2019 Annual Report*. Wellington: New Zealand Government, p. 21

Annexure 1 – Background on Standards Australia

Standards Australia is recognised by the Commonwealth as Australia's peak non-government standards body. Founded in 1922, it is an independent and not-for-profit organisation and is the Australian member of the International Organisation for Standardisation (ISO), International Electro technical Commission (IEC) and the Pacific Area Standards Congress (PASC). At the international level, Standards Australia is committed to representing the views of stakeholders, government and consumers in standards development and related activities. Domestically, standards are developed for the net benefit of Australia and enhance economic efficiency, increase community safety and sustainability, and improve industry and international competitiveness.

Standards Australia facilitates standards development through technical committees, by bringing together relevant stakeholders to develop standards documents through a process of consensus. Our current catalogue consists of approximately 6000 voluntary standards across 12 sectors of the Australian economy, including energy and electrotechnology, ICT, manufacturing and consumer products and services. The building and construction sector is a standards development priority for Standards Australia and involves engagement with legislative authority at all levels of Australian government.

Standards Australia works with all tiers of government and industry. Our standards development process creates opportunities for a robust exchange of knowledge, expertise, and perspectives in the development of consensus based standards and other solutions to improve performance, productivity, as well as health and safety outcomes for all Australians.