Standards Australia Limited
Exchange Centre, Level 10, 20 Bridge Street, Sydney NSW 2000
GPO Box 476, Sydney NSW 2001
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

31 October 2019

Mr James Robinson
Director – Emerging Technology and Market Reform
Australian Cyber Security Centre
Department of Home Affairs
CANBERRA ACT 2601

Department of Home Affairs
Via email to: cybersecuritystrategy@homeaffairs.gov.au

Dear Mr Robinson

RE: AUSTRALIA'S 2020 CYBER SECURITY STRATEGY – A CALL FOR VIEWS

Standards Australia welcomes the opportunity to provide this submission to the Department of Home Affairs regarding the development of Australia's *2020 Cyber Security Strategy*. We seek to respond only to matters that are considered relevant to our work and engagement as Australia's peak standards development body.

Standards Australia is responsible for overseeing the development of Australian Standards, and the adoption of International Standards through ISO and IEC, that can provide solutions for increased uptake of cyber security solutions. Our intent is to widen and deepen our engagement in cyber security, an important issue for the Australian community.

We acknowledge the significant work undertaken by the Australian Government, including through the Australian Cyber Security Centre (ACSC) and AustCyber, to improve cyber security practices, threat detection and co-ordination efforts, and grow the market.

The Australian Government's *A Call for Views* consultation paper included a range of questions. Standards Australia wishes to provide the following recommendations in response to the following questions raised by the consultation paper:

- Question 12 - *what needs to be done so that cyber security is 'built in' to digital goods and services?*
- Question 26 - *is there anything else that the Government should consider in developing Australia's 2020 Cyber Security Strategy?*

Recommendations

1. The Australian Government agree to participate, via Departmental representatives, in a Standards Australia Chairs Advisory Group (CAG) on Emerging Technologies.
   They would meet at agreed intervals and provide updates on progress in standards development internationally, in areas including, but not limited to: Artificial Intelligence, Cyber Security, Blockchain, and International Strategic Advisory Committee.

2. The Australian Government, through the Department of Home Affairs (and specifically the ACSC), consider formally participating in the International Strategic Advisory Committee and international work of Cyber Security.

Standards Australia Limited
Exchange Centre, Level 10, 20 Bridge Street, Sydney NSW 2000
GPO Box 476, Sydney NSW 2001
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

3. The Australian Government support and resource a joint initiative between Standards Australia and AustCyber to facilitate the adoption of International Standards such as the international 27000 series of Standards, and relevant Australian Handbooks.

4. The Australian Government support a mapping exercise to identify relevant legislation, regulation and cyber security standards (such as National Institute Standards Technology, Information Security Manual and Protective Security Policy Framework) to highlight any gaps or overlaps with International Organization for Standardization (ISO).

Enhancing Australia's participation in cyber security standards setting internationally

Standards have a long history as part of Australia's security architecture, for both the private and public sector. Part of the drive to use Standards is to meet existing regulatory or policy requirements, where they are referenced as a technical means to satisfy regulatory objectives.

This might include in the financial services sector or in government agencies. For example, AS ISO/IEC 27001 (Information Security Management) is widely used within Australian financial institutions, including banks, to ensure appropriate controls are embedded at an enterprise level, to protect personal information. Additionally, some Government Departments, or whole-of-government frameworks[1] require certification against Standards, such as AS ISO/IEC 27001 as a baseline requirement, in the absence of which variable security practices might otherwise exist.[2]

It is important to note that protective security, aside from information security and other critical aspects, comprises a critical component of overall cyber security. The Attorney General's Department, through the *Protective Security Policy Framework,* for example, references International Standards and Handbooks, as supporting material for organisations, focusing on physical protection of key assets:

- *AS ISO 55001:2014 – Asset management – Management systems – Requirements*
- *AS 4811:2006 – Employment Screening*
- *HB 323:2007 – Employment Screening Handbook*
- *AS/NZS ISO 31000:2018 – Risk Management – Guidelines*
- *HB 167:2006 – Security Risk Management*
- *HB 327:2010 – Communicating and consulting about risk*
- *HB 158:2010 – Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines*
- *ISO Guide 73 – Risk Management – Vocabulary*
- *AS 3745:2010 – Planning for emergencies in facilities*
- *AS/NZS 4801:2001 – Occupational Health and Safety Management Systems*
- *AS 5815:2010 – Protocol for lightweight authentication od identity (PLAID)*
- *AS 4421:1996 – Guards and patrols*
- *AS 4145.2:2008 – Locksets and hardware for doors and windows – Mechanical locksets for doors and windows in buildings*

---

[1] As an example, see reference to ISO 27001 in: NSW Government. (2019). 'Cyber Security Policy'. Accessed: 09/06/2019 from: https://www.digital.nsw.gov.au/policy/cyber-security/cyber-security-policy See also: Biscoe, C. (2019). 'ISO 27001 growth in Australia stems from government initiatives', accessed 16/10/2019 from: https://www.itgovernance.asia/blog/iso-27001-growth-in-australia-stems-from-government-initiatives

[2] Audit Office of NSW (2018). *Detecting and responding to cyber security incidents.* Sydney: Audit Office of NSW.

Standards Australia Limited
Exchange Centre, Level 10, 20 Bridge Street, Sydney NSW 2000
GPO Box 476, Sydney NSW 2001
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

- *AS 4806:2008 – CCTV suite, which includes*[3]

Standards can also be used, through private contractual means, to manage risk and reduce liabilities. For example, the adoption of standard controls throughout a supply chain, might enable a primary contractor to better meet their own contractual obligations and to provide a baseline level of assurance that services provided are secure. This can have positive market spill-over effects too, raising the bar when it comes to cyber awareness and, critically, cyber secure practices, embedded daily.

In order to ensure that International Standards on cyber security remain fit-for-purpose, the Australian Government, through Home Affairs (and specifically the ACSC), and other relevant Government departments, should give consideration to increasing their levels of participation in Standards development activities. We note the increasing engagement occurring between national government and standards development organisations, including in the United Kingdom, the United States and Singapore.

With support from the Commonwealth Government *Support for Industry Service Organisations* program, Standards Australia is responsible for coordinating the attendance of Australian experts at International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) meetings. In areas related to information security, cyber security and privacy protection, there are a range of international technical committees developing Standards.

We note the comments of Prime Minister, The Hon. Scott Morrison, MP, observing,

"When it comes to setting global standards, we've not been as involved as we could be. I'm determined for Australia will play a more active role in standards setting."[4]

Standards Australia is of the view that this could extend to cyber security and standards around emerging digital technologies more broadly. This is consistent with earlier policy statements emanating from the Australian Government. *Australia's Tech Future*, released in late 2018 by the Department of Industry, Innovation and Science (DIIS), cites, as one of its objectives: "Global rules and standards affecting digital technologies and digital trade support Australia's interests."[5]

Additionally, in the area of emerging technologies, Australia has committed itself, alongside 41 other countries, to the *OECD Principles on AI*. This explicitly calls for Governments to "promote the development of multi-stakeholder, consensus-driven global technical standards for interoperable and trustworthy Artificial Intelligence."[6]

The importance of industry and government alignment in these areas of emerging digital technologies is underlined by the moves by countries with which Australia enjoys formal alliances, including the United States and United Kingdom, to formally map Standards activity required, in collaboration with industry, and through National Standards Bodies. As an example, this has been mirrored in Australia by the development of an AI Standards Roadmap, by Standards Australia.[7]

---

[3] Attorney General's Department (2019). 'Relevant Australian and International Standards', accessed 15/10/2019 from: https://www.protectivesecurity.gov.au/resources/Pages/relevant-australian-and-international-standards.aspx
[4] As quoted in Coorey, P. (2019). 'Unchecked globalism and threat to Australia's sovereignty', *Australian Financial Review* (October 3rd).
[5] Department of Industry, Innovation and Science (2018). *Australia's Tech Future: Delivering a strong, safe and inclusive digital economy*. Canberra: Commonwealth of Australia, p.45
[6] Organization for Economic Co-operation and Development (2019). *Principles on Artificial Intelligence*. Paris: OECD.
[7] Standards Australia (2019). *Artificial Intelligence: Hearing Australia's Voice*. Sydney: Standards Australia.

Standards Australia Limited
Exchange Centre, Level 10, 20 Bridge Street, Sydney NSW 2000
GPO Box 476, Sydney NSW 2001
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

To facilitate greater engagement by the Australian Government in these areas, Standards Australia proposes to establish an internal Chairs Advisory Group (CAG) for emerging digital technologies, with a remit to focus on cyber security standards. The Australian Government, including through Department of Industry, Innovation and Science (DIIS) and Home Affairs (ACSC) will be invited to participate in meetings, scheduled twice a year.

The purpose of this CAG is to provide a comprehensive 'birds-eye' view of Standards development activities to the Australian Government, so they can anticipate issues, opportunities for engagement and pathways to influence and advance Australia's interests, as appropriate.

Building capacity and scaling businesses through Standards

Standards can function as market enablers, as well as means to achieve broader business and public policy goals around raising cyber security awareness. Standards can enable the growth of businesses, as globally-embedded norms that service providers can build to, as they expand into new markets where adherence to International Standards (such as ISO/IEC/27001) might be beneficial.

In the United Kingdom, for example, many companies, including small and medium-sized businesses build to the requirements of Standards to enable them to sell their services to both governments and the private sector.[8] This requires a clear awareness of the technical requirements of Standards (including controls) and how to implement them at-scale, as well as knowledge of certification processes.

Beyond Standards development, there are also opportunities to help position Australian cyber security providers as market leaders regionally and globally. Through a collaborative initiative between Standards Australia and industry, such as AustCyber, we can facilitate access to Standards, and identify opportunities to assist Australian businesses modernise and implement cyber security capabilities. AustCyber are the Growth Centre for the cyber industry in Australia. They have a track record of collaborating with SMEs and larger companies in the cyber security arena, to build the cyber security eco-system. Their insights position them uniquely to contribute to a joint initiative to improve the uptake and use of cyber security-related Standards in the Australian market, in a language, and through an approach, that is market friendly and also meets business needs.

Further contact

Our Strategic Advocacy Manager, Dr Jed Horner, would welcome the opportunity to brief you on our standards work and our recommendations. Jed can be contacted by phone on [redacted] or by email [redacted]

Yours sincerely

[redacted]

Daniel Chidgey
Head of Stakeholder Engagement

[8] See, for example: United Kingdom Government (2019). 'FlyingBinary Ltd: IoT Smart City Sensor Analytics' https://www.digitalmarketplace.service.gov.uk/g-cloud/services/170499651495382

Standards Australia Limited
Exchange Centre, Level 10, 20 Bridge Street, Sydney NSW 2000
GPO Box 476, Sydney NSW 2001
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

Appendix

Standards Australia: Who we are and what we do

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 Organization for Standardization (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 & 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, industry and the wider Australia community, such as The Australian Industry Group, Engineers Australia and others. 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.