RECOMMENDATIONS REPORT

# NSW Cyber Security Standards Harmonisation Taskforce

# Contents

# Introduction: Tackling cyber risk in the digital age – Creating a 'rising tide' to lift all boats

The risks we face are changing and amplifying in our digital world. Cyber physical systems, common digital architecture like cloud services and the rise of connectivity at-scale, all present considerable social and economic opportunities. But, they also present increased risks. These cyber security risks span both the macro and micro economic contexts, such as what would occur if critical systems were compromised, leading to loss of services or lives, through to theft of an organisation's intellectual property, or the disclosure of sensitive information or personal data.

Addressing these risks through the adoption and use of common standards has been the focus of the NSW Cyber Security Standards Harmonisation Taskforce. This is not intended to imply that standards are a panacea to these risks. They are not. Rather, used in combination with the latest advances in technology, and embedded across global supply chains, they can assist in raising the cyber security posture of a small to medium enterprise (SME), organisation or government agency in market and internationally. Importantly, as you will observe in reading the recommendations of this Taskforce, this posture is not always about technical controls, but equally about protective security.

It is often said in cyber security that people can be the weakest link. We agree. Without adequate protective security measures – ranging from the physical security of facilities to personnel screening – it is unlikely that efforts to raise the bar when it comes to cyber security will succeed to the full extent possible. The challenge here, is embedding approaches across industry and government in a way that achieves a degree of uniformity, provides confidence and demonstrates an ongoing cyclical process of review, assessment and rectification. Perfection, after all, is an art form we continually strive towards.

There are logical connections here with existing and proposed regulatory reforms. The Australian Government, following other governments, is making new investments in cyber security measures and capabilities, and proposing regulatory reforms in relation to critical infrastructure. In the past, similar cycles of regulatory activity have provided ample opportunity to consider what the policy goals we are trying to achieve are, to align practical frameworks to these goals, and finally, to ensure that International Standards developed, adopted and leveraged, are consistent with these. This remains contingent on industry engagement. As a result, we sincerely hope that, during the current era of reform, the deep expertise that exists within industry is harnessed to achieve an improved overall cyber security posture for our collective benefit.

Finally, we thank the generous, constructive and energetic contributors from the NSW Cyber Security Standards Harmonisation Taskforce, from across industry, government and academia who helped shape this Recommendations Report.

—**Prerana Mehta**
Chief of Ecosystem Development,
AustCyber

—**Dr Jed Horner**
Strategic Advocacy Manager,
Standards Australia

AustCyber
Australian Cyber Security Growth Network

STANDARDS Australia

# CEO forewords

## Standards Australia

It is my pleasure to launch the Recommendations Report of the NSW Cyber Security Standards Harmonisation Taskforce. This Taskforce, comprising of industry, government and other representatives, worked diligently to arrive at a series of practical recommendations to improve our cyber security posture.

We are appreciative to both the NSW Government and AustCyber for this partnership – which reflects a joint commitment to working openly and collaboratively in a common area of interest.

As Australia's national standards body, we look forward to working with stakeholders to advance these recommendations, ranging from guidance material, to revisions to standards. We also call on government and industry stakeholders to ensure that we leverage international standards as the Australian Government shapes new requirements for cyber security in Australia, across a range of sectors of the economy.

To those of you who have contributed, we thank you and look forward to continuing to work with you.

—**Adrian O'Connell**
CEO Standards Australia

## AustCyber

The Australian cyber security sector is rapidly maturing. It is well positioned to enable the uptake and application of trusted digital technologies and practice to promote economic growth and recovery.

AustCyber's mission is to grow a robust and globally competitive cyber security sector that delivers economic security benefits. Cyber security standards play a key role in improving the security of data, assets, systems, networks and critical infrastructure. Well-developed, practical and verifiable standards enable consistency and encourage competitiveness among developers and organisations.

We are pleased to have partnered with the Hon. Victor Dominello, Minister for Customer Services, NSW Government and Standards Australia in leading a taskforce of industry groups to identify and adopt common standards for cyber security across Australia. These recommendations and the subsequent framework of harmonised baseline standards will provide clarity and guidance for sector-specific application and adoption of cyber security standards and certification – delivering growth and a more resilient national economy.

Our partnership with the Minister and NSW Government on implementing best practice approaches to cyber security, as an exemplar for the nation, takes a three-part approach. Standards and clear guidance to improve business maturity around cyber risk is complemented by taking steps to address barriers for local innovative cyber security companies accessing NSW government procurement opportunities; and taking a networked effect to delivering cyber security jobs and support for SMEs across regional NSW. These are the foundations for government providing leadership in building cyber resilience and growing retained economic benefit from a critically important industry.

I encourage industry and all levels of governments across the country to review and implement the recommendations outlined in this report. Ultimately, a globally competitive Australian cyber security sector will underpin the future success of every industry in the national economy. Together, let's foster innovation and generate increased investment and jobs through the creation and commercialisation of cyber security products and services, utilising agreed standards to build a more secure Australia.

—**Michelle Price**
Chief Executive Officer, AustCyber

# Ministerial Overview

I am pleased to present the Final Report of the NSW Cyber Security Standards Harmonisation Taskforce.

When I established the Taskforce, I knew it would be a critical step in bolstering our collective cyber security resilience and helping to create a strong NSW cyber security ecosystem. This report demonstrates that when we commit to tackling difficult problems, they can be managed in a fast and agile manner despite the complexity of the task.

Cyber security is no longer an issue reserved for information security departments. Digital infrastructure is at the heart of driving Australia's recovery from the COVID-19 pandemic and cyber security functions are an insurance policy for a resilient economy.

As consumers, business owners and citizens, we all need assurance that the products and systems we use are secured to the highest industry standards. In order to achieve this, we needed to simplify the range of current security standards. By having an ever-growing plethora of different standards, it was difficult for governments and industry to know what they were buying in regards to cyber security.

Through the concerted effort of the Taskforce, standards have been mapped out. This will be an invaluable tool as government works to be even more secure, whilst providing direction for industry to build their cyber resilience. This will undoubtedly help businesses understand what they need to do to tackle the complex challenge of protecting against cyber attacks.

I would like to thank the industry participants who, as members of the Taskforce, volunteered their time, expertise and passion over the past six months.

I would also like to thank, in particular, AustCyber and Standards Australia. Their commitment and insights have helped drive the Taskforce to arrive at the Recommendations Report.

—**The Hon. Victor Dominello MP**
NSW Minister for Customer Services

# High-level insights for policy and practice

01 There are a myriad of cyber security standards to select from. Some standards (i.e. ISO, IEC, EN, NIST) are embedded into policy and assurance frameworks and others are not.

02 Good practice will differ between sectors, in relation to entity size, threat surface, risk appetite, maturity and customer orientation.

03 Care must be taken to factor-in how standards are to be used, for what purposes and in relation to specific public policy requirements. This might include consideration of the relative merits of principles-based approaches, attestation, certification and how development, adoption or use of standards might impact supply chains or procurement behaviour.

04 The quality and volume of guidance material on implementation of specific standards needs to improve. This includes how the material maps to government frameworks (existing or proposed).

05 A cyber security workforce skills gap exists in relation to understanding and application of standards and compliance.

06 Some targeted government support might be required for specific growth sectors (i.e. to support market entry in more complex markets and where there might be a significant return on investment).

## Making standards information accessible – an online resource

The Taskforce agreed it was important to provide a publicly accessible list of standards relating to cyber security, across the seven sectors that were the focus of its work. For this to be useful, whether for businesses, governments or researchers, it additionally needs to map core legal and regulatory requirements in those specific sectors, and how they might interact with standards. In early 2021, this work will be completed, following initial consultation with Taskforce members in late 2020.

# Recommendations – at a glance

Several recommendations are provided in this report, relating to seven key sectors. The overarching insights, and areas for action, include the following:

01

**New practical guidance material across all sectors is needed.**

This might include:

a. How to select standards, relative to entity size and risk appetite.
b. How to implement standards, with reference to specific use-cases.

02

**Revision of certain existing standards is warranted.**

This might include:

a. Where circumstances warrant a greater cyber focus (i.e. asset management).
b. Where cyber hygiene practices evolve, presenting an opportunity to update the baseline (i.e. during scheduled ISO/IEC review cycles).

03

**Considered use of standards in policy and regulatory responses is important.**

a. Leverage recognised international standards, understanding that businesses often spend significant resources implementing these.
b. Beyond narrowly mandating standards, referencing or providing a weighting relevant to their application, particularly in relation to procurement processes, can be useful.

## Priority area: Digital backbone – cloud

- Cloud platforms are essential to building micro-services and to enable cost effective scaling for government and businesses. Cumulative productivity benefit of cloud adoption to the economy was A$9.4 billion over a five year period.[1]
- Cloud providers already use a range of recognised International Standards and meet an array of legal requirements, across borders.
- Specifying and leveraging commonly used, and globally recognised, Standards is essential to ensuring the benefits of cloud are realised and maturity horizons for security are met.
- Australian government agencies, as well as private sector partners, can leverage these international standards (and existing conformance testing and certification processes) to specify requirements, streamlining compliance and reducing costs for government and customers alike.

### Recommendations

01 Australian governments should adopt and leverage recognised ISO and/or IEC Standards as baseline requirements for information security (i.e. ISO/IEC 27000 series), protective security (i.e. ISO 22340, forthcoming) and supply chain security and risk management (particularly ISO 28001 and ISO 31000), through any regulatory frameworks or procurement models proposed in relation to cyber security. In the event that a principles-based approach is adopted, this should be consistent with these recognised International Standards, and enable businesses to leverage their existing compliance or identify a maturity lift required from this baseline, rather than creating duplicative requirements at cost to business and the broader community.

02 Australian governments, in relation to any new proposed cloud security requirements for services up to, and including, PROTECTED level, should consider a combination of compliance with ISO/IEC 27001, SOC 2 and potentially FedRAMP[2] as part of a uniform security baseline.

03 Australian businesses and governments, should, through Standards Australia, develop material, in open or handbook form, that clearly communicates any business benefits around the adoption of standards, categorises applicable standards that might apply in specific settings, and the importance for boards, executives and relevant decision-makers of their use. This information should be as clear as possible, grounded in case studies on:

a the importance of standards for trade and transnational commitments;
b the benefits of risk-based frameworks and controls across enterprises and partner/supplier chains and;
c how businesses of different sizes implemented these approaches in real-world settings

1 Deloitte Access Economics (2019). The Economic Value of Cloud Services in Australia.
2 The Federal Risk and Authorization Management Program (FedRAMP) is a US Government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

## Priority area: Defence

- Over the next ten years, the Australian Government will provide Defence with total funding of around $575 billion.[3] This includes significant capital expenditure.
- Baseline cyber security will likely underpin most of this expenditure, including procurement, design and sustainability.
- There is a growing appetite to strengthen Australia's capabilities to more actively participate in global supply chains, including through specified on-shoring requirements for new acquisitions. The defence sector is a priority growth area for several states and territories including NSW.
- Australia needs to be mindful of its defence alliances and ensure that any domestic focused standards or certification requirements (new or developing) consider those that are already in existence in other markets. These range from specific defence requirements, through to security for 'horizontal' and supply chain providers particularly in relation to cloud[4].
- The Cyber Security Maturity Model Certification (CMMC), from the United States, is of particular interest and efforts should be made to harmonise requirements to the furthest possible extent.
- An approach based on effective risk identification, analysis, management and treatment was viewed favourably by participants.

### Recommendations

01 The Australian Government should explore how CMMC alignment will take place, and ensure that new arrangements enable Australian suppliers to meet requirements in an appropriate and, ideally, expedited manner.

02 The Australian Government, as well as state and territory governments, should develop material that clearly communicates any business benefits, as well as practical realities of implementation, concerning specific legal and regulatory requirements, including internationally applicable laws, as well as local frameworks and directives of relevance (i.e. DSPF and PSPF), and how recognised International Standards intersect.

03 Businesses, and other stakeholders, should consider the development of an Australian Interim Standard or Technical Specification, through Standards Australia, outlining how to develop an information security strategy as envisaged under ISO/IEC 27014:2013, *Governance of information security*.

04 Australian businesses and governments, through Standards Australia, should consider adopting ISO 22340, *Protective security – Guidelines for an enterprise protective security architecture and framework*, upon publication, as an Australian Standard, to provide a risk assessment and treatment approach in relation to protective security. This new draft Standard, currently out for consultation, is benchmarked against our respective protective security requirements.

05 Australian businesses and governments, through Standards Australia, should explore the extent to which AS ISO 55001, commonly referenced in procurement, and specifically in relation to sustainment, can explicitly take into consideration cyber security requirements. This might be through an amendment locally or

3 Source: 2020 Defence Strategic Update
4 See, for example: https://www.fedramp.gov/

internationally, in accordance with the established ISO review cycle for published Management System standards.

06 Australian businesses and governments, through Standards Australia, should explore the application of the revised ISO 28000, *Supply Chain Security* and the ISO/TS 22381, *Supply Chain Business Continuity Standards for cyber security requirements.*

07 Australian businesses and governments, through Standards Australia, should consider revisions to handbook HB 167:2006 - Security Risk Management, which provides detailed contextual information, to ensure it remains relevant, is adequately illustrative of good practice and meets evolving needs. There might also be an opportunity for greater alignment with the PSPF and other relevant frameworks and directives.

5 **London Economics (2018). The Economic Impact of Group of 8 Universities*

## Priority area: Education

- The education sector is vital to Australia's economic wellbeing. A 2018 analysis found that Group of 8 Universities alone contributed A$66.4 billion to the national economy in a single year through a range of flow on effects.[5]
- Cyber security at universities is about more than just software and hardware, and includes protective security. The focus within universities is on protecting personal information, IP developed by researchers, and controlling the export of dual-use technologies, whilst delivering on commitments, including those outlined in joint ventures.
- Participants expressed their preference for risk-based frameworks that can be adapted for entity size and risk appetite at an institutional level, including NIST CSF and ISO 27001.
- Guidance material was identified as important, illustrating the 'how to' and emphasising the role of communication, rather than developing too many new regulatory requirements in an evolving area, where research and partnerships are often pertinent to national and emerging priorities. This includes areas that are already heavily regulated due to their sensitivity.

### Recommendations

01 Education stakeholders should develop clear guidance material that highlights the benefits of different risk-based frameworks in existence. This would be a document that enables people to understand and manage their risk exposure, select their model, based on clear case studies drawn from real-world applications within educational contexts in Australia. The intended audience would be educational institutions, primarily universities.

02 Education stakeholders, through Standards Australia, should develop an Australian Technical Specification on reporting cyber vulnerabilities, which can be trialled, tested and validated in Australia, and leveraged as a basis for future ISO/IEC standardisation internationally. This could leverage US Homeland Security Binding Operational Directive 20-01, as well as related ISO Standards such as ISO/IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*.

03 Education stakeholders, through Standards Australia, should consider revisions to Handbook HB 167:2006, Security Risk Management, to ensure it remains relevant, is adequately illustrative of good practice and meets evolving needs. This might include new material relating to 'insider threats' and protecting dual-use IP and materials within educational contexts.

## Priority area: Energy

- The energy sector is heavily regulated, including at state & territory level, through relevant licensing agreements and legislative frameworks.
- The sector are heavy consumers of International and Australian Standards, as well as broader risk management frameworks. AEMO's recently released Australian Energy Sector Cyber Security Framework (AESCSF) is widely recognised as a risk-based approach to improving the cyber posture of the sector.
- Open energy networks could and should warrant further focus. Internet of Things (IoT) is a key area of focus, given the increasingly distributed nature of energy generation and distribution.
- Governments and others involved in this sector must be cognisant of state level requirements in introducing new frameworks and approaches, as well as business impacts of new requirements in light of fiscal restraints in terms of what operators can pass on to customers.

### Recommendation

01 Develop material that clearly communicates any business benefits around the adoption and use of standards to improve cyber security posture in the energy sector, and the importance for boards and executives, in particular. This should include in relation to managing their legal obligations (for example, the Corporations Act, as well as energy-specific statutes) and the information should be rendered as clearly as possible.

## Priority area: Financial services

- The financial services sector has traditionally been an area of strong growth and performance in Australia. It is heavily regulated, ensuring risk and compliance including in cyber security.
- Specific standards of note include APRA 234, a risk-based framework which entities are audited against at specific intervals, SOC 2 and PCI-DSS (across entities).
- More recently, the Consumer Data Right is being rolled-out within Australia and specific nominated sectors, with specific requirements.
- There is scope to reach international agreement on technical data standards for consumer data sharing, through recognised international standards bodies (i.e. ISO, IEC) if the uptake in Australia is sufficient and there is multilateral interest and agreement.

### Recommendations

01 Australian governments should consider formally participating in the Standards Australia Mirror Committee to SC 27, which develops the ISO/IEC 27000 suite (ranging from Management System standards through to guidance material). This is to ensure future revisions to commonly used Standards reflect any wide-scale changes in regulator and market requirements.

02 Australian Governments, Standards Australia and others embed material about PCI-DSS application in material across sectors, owing to its common use. This might be through illustrative handbooks, for example.

03 Stakeholders, including designated sectors, could explore which elements of the CDR work best in practice. On this basis they could propose a New Work Item through ISO and/or IEC (i.e. JTC 1), to expand the scope and reach of this approach, contingent on wider agreement.

## Priority area: Health

- The Healthcare sector is already the fifth largest contributor to Australia's GDP, and accounts for a significant employment footprint[6].
- Exports are critical to the growth of the sector, whether in terms of products or services. Underpinning infrastructure, such as cloud, is also essential to the growth of this sector, particularly in relation to services.
- The healthcare sector is already one of the most heavily regulated in Australia, at both state and Commonwealth levels. However, it is often complex to navigate with lack of clarity around specific sub-sector requirements.
- International Standards, including those adopted in-market (specifically ISO, IEC and EN Standards), are often a requirement to entry overseas, tied to either product or service compliance (i.e. quality control, security, safety).
- Requirements for compliance keep increasing, as do resulting costs, but there is a skills and knowledge gap in relation to legal frameworks, and Standards compliance and, in some senses, a funding gap - particularly for entry to specific markets when it comes to medical devices.
- There is an opportunity for a capability uplift in the health area when it comes to Standards (specifically related to medical devices), through government support and investment.

### Recommendations

01 Australian businesses and governments, through Standards Australia, should develop material such as handbooks or playbooks, that clearly communicate any business benefits around the use of recognised international standards to better meet legal and regulatory requirements, and the importance for boards and executives, in particular. This information should be made as clear and grounded in case studies as possible, particularly market entry for particular segments in specific priority markets.

02 Australian governments should ensure that any future guidance on cloud that they develop or mandate, as foreshadowed by proposed Critical Infrastructure reforms, takes a maturity-based approach, which factors into consideration entity size in relation to risk profile, and recognises the centrality of Standards such as ISO/IEC 27001, SOC 2, FedRAMP.

03 Australian governments, including the NSW Government, should explore the provision of additional support for market entrants to improve access to certification or standards advisory services in strategic areas, such as cyber readiness for Medtech, to support export growth. This might take the form of targeted vouchers or grants, or supported advisory programs. This support could be supported by a formalised assessment process that also takes into account expected Return-On-Investment.

---

6 *PWC (2016). Australia's Healthcare System: An Opportunity for Economic Growth.*

## Priority area: Telecommunications & IoT

- As a sector, telecommunications is already heavily regulated in Australia, with maturity and granularity in terms of regulatory approaches.
- IoT is an area attracting attention in terms of standardisation, including in relation to security vulnerabilities.
- There are a range of Standards Development Organisations (SDOs) operating in this area and at different levels. More coordination here is vital and this should be international in scope.
- There are opportunities to encourage greater adoption and use of standards within supply chains, including within government decision-making.

### Recommendations

01 Australian governments, in creating new digital policy documents and/or directives, should require agencies to explicitly consider cyber security considerations, including recognised standards, in their development and later adoption. This might, for example, be prior to Cabinet or Expenditure Review Committee consideration.

02 Australian governments should explore mechanisms to consider, and weight, proposals or tender bids that demonstrate company-wide consideration and adoption of recognised International Standards in relation to cyber security, risk management, and where appropriate, IoT security more specifically. This could occur, for example, through assurance processes with routine reporting on the percentage of vendors who demonstrated that they met the requirements of particular standards. It could also include prioritising proposals or tender bids which demonstrate compliance with recognised international standards or codes.

03 The Australian Government should consider convening a multi-stakeholder IoT Working Party, to meet at agreed intervals, share information on new proposals and ensure alignment in relation to the development of core, and supporting, IoT Standards across ISO, IEC, the ITU and other fora, including private sector consortia.