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

27 February 2024

Department of Home Affairs
By email: AusCyberStrategy@homeaffairs.gov.au

Dear Sir/Madam

Re: 2023-2030 Australian Cyber Security Strategy: Legislative Reforms CONSULTATION PAPER

Standards Australia (SA) is pleased to provide a submission to the Australian Government's 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper.

Introduction

The increased adoption of smart devices, also known as Internet of Things (IoT) devices, is a positive step towards creating a technologically enabled nation. However, these consumer-grade smart devices can expose citizens to potential cyber incidents. Smart devices are pervasive in society and whilst traditionally not considered vulnerable to cyber-attacks, they can expose Australian citizens to cyber threats and incidents not previously experienced. Embracing IoT technology which is secure-by-design is crucial for consumers to understand in order to create a culture of safety. SA supports the Australian Government's Cyber Security Strategy (the Strategy), and is committed to helping build support, trust, and consensus amongst relevant stakeholders for activities in support of the Strategy. SA can support the Australian Government to adopt and develop, internationally aligned foundational standards to establish a consensus-driven approach to cyber security that is complementary to regulation.

SA is pleased to provide input into the Consultation Paper, specifically the proposed mandatory product standard for consumer-grade IoT devices in Australia under initiative 8 of the Strategy. SA also supports the proposed Voluntary Labelling Scheme for consumer-grade IoT devices.

As Australia's peak not for profit standards body and the representative for Australia on a global platform within ISO and IEC, our recommendation would be for the Australian Government to work with SA to establish the mandatory standard. Through our consensus driven approach and extensive reach amongst stakeholders from industry, academia, and government, SA can design a process that allows Australia to leverage the work already done. Extensive standards work has been done already in cybersecurity internationally, nationally, regionally and within industry already to provide a mandatory standard which is suitable for the Australian context. Standards curation requires a broad spectrum of stakeholders and an international understanding and lens to ensure regulatory compatibility and interoperability as well as security within other jurisdictions. The SA approach would ensure that Australia does not duplicate effort in developing a mandatory standard but understands the necessary requirements for the Australian context and utilises existing work done internationally. SA would look to the work done internationally particularly UK (PTSI), US (Executive Order 14028) and Singapore.

The Australian Government has worked closely with SA processes to develop national referenced standards for MEPS (Minimum Energy Performance Standards), GEMS (Greenhouse Energy Minimum Standards), WELS (Water Efficiency Labelling and Standards) and, significantly, the National Construction Code (Building and Plumbing Code) and Watermark product certification in close and careful collaboration with the Australian Building Codes Board.

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

SA's processes are well-established and take a best-in-class curated approach to standards development. We hold a Memorandum of Understanding with the Commonwealth, and our policies align with the Australian Building Codes Board's via their Protocol for Development of Referenced Documents. Use of SA's referenced standards facilitates the minimum requirements of the National Construction Code's performance-based building and plumbing code.

SA have also engaged with ACCC on several of their draft guidance and mandatory standards, the most recent being to assist businesses making environmental claims. In this instance, SA were able to turn to ISO 14020 Environmental statements and programmes for products — Principles and general requirements, and its related suite of Standards to provide valuable information designed to assist the regulator in creating this policy.

Voluntary labelling scheme for consumer-grade IoT devices

The Australian Government play a crucial role in raising awareness and promoting cyber secure consumer grade IoT devices, as such SA support the proposal to develop a voluntary labelling scheme. Labelling schemes can increase consumer confidence and purchasing power, to provide consumers the ability to determine which IoT devices are protected. Many labelling schemes are harmonised with standards to guide manufacturers on how to accurately rate and label their products cyber safe without making false claims. The Water Efficiency Labelling Standards (WELS) trust mark scheme is a good example of an existing standards-based scheme which SA was involved in developing. SA support this initiative under the Strategy and recommend the Australian Government engage SA and IoTAA as partners.

Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?

SA believe that compliance with the proposed mandatory cyber security standard at a minimum should be extended to anyone who is a supplier or contractor to the Australian Government. This aligns with NIST's Compliance with Cybersecurity and Privacy Laws and Regulation and the UK Government's Minimum Cyber Security Standard. In addition, manufacturers and retailers who operate within commercial supply chains should be required to adhere to a mandatory cybersecurity standards for consumer-grade IoT devices.

Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?

SA believes that the first three principles of the ETSI EN 303 645 standard are an appropriate minimum baseline for consumer-grade IoT devices sold in Australia. ETSI EN 303 645 has already been adopted in Australia by SA and was published Nov 17, 2023 and assessed as relevant to the Australian context by the committee (IT-012 Information Systems, Security & Identification Technology).

What alternative standards, if any, should the Government consider?

SA encourages the Australian Government to consider other international cybersecurity standards in addition to ETSI EN 303 645 to meet regulatory requirements. SA would recommend the Australian Government collaborates with SA on a standards mapping exercise to identify additional mechanisms to achieve cybersecurity safety and interoperability. These mechanisms may include performance-based frameworks which could support compliance through a deemed-to-satisfy approach that offers greater flexibility. Cybersecurity frameworks and standards already exist which support this effort, SA can help identify those and engage stakeholders to curate and inform the Australian Government on which standards would be most applicable to the Australian

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

context. SA suggest supporting the Australian Government in determining equivalent standards to ETSI EN 303 645 which might also meet regulatory objectives (IEC 62443-4-2, ISO 21434, NIST IR 8425, UK PSTI, RED 3.3 (d.e.f.)).

Recommendation

SA have provided an Annex to support these views which provides further insights on recent and current efforts on cybersecurity on a national and international scale through standards and to illustrate the importance of standards.

Recommendations:

1. The Australian Government work with SA and industry experts through consultation to develop and deploy a mandatory standard for consumer-grade smart devices in Australia.
2. The Australian Government work with SA on a standards mapping exercise for consumer-grade IoT devices to understand the existing standards landscape and scope opportunities to become standard-setting in new fields of consumer-grade cybersecurity.
3. The Australian Government to work with SA and the IoTAA to develop, consult and co-design a voluntary labelling scheme for consumer grade IoT devices which will be interoperable with a mandatory standard.
4. The Australian Government to work with SA to continue to support the development of industry-based cybersecurity standards through multilateral systems such as ISO/IEC.
5. The Australian Government to work with SA on supporting the proposed amendments to the SOCI Act in relation to data storage systems held by critical infrastructure.

We look forward to the opportunity to discuss the submission in further detail. Please contact Soraya Selinger, Strategic Initiatives Manager, at [redacted]

Yours sincerely

[redacted]

Adam Stingemore
Chief Development Officer

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

Annex 1: Background to the Submission

Supporting mandatory standards development

The establishment of approaches to supporting mandatory standards requires the development or adoption of appropriate national and international standards.

Cybersecurity standards development

SA is responsible for overseeing Australian Standards® development, and the adoption of International Standards through the International Standards Organisation (ISO) and International Electrotechnical Commission (IEC). We work with industry, government, and the community to develop and adopt standards through an open process of consultation and consensus. We invite interested parties to participate in these processes.

Our intent is to widen and deepen our engagement in supporting cybersecurity standardisation, which we recognise as important enabling technologies for resilient communities and as critical drivers for Australia's future prosperity.

We view international standards, through ISO and IEC, as a sensible pathway to supporting international norms that facilitate the development of cybersecurity systems that are fit for purpose and benefit society.

International standards can function as market enablers, and a means to achieve broader business and public policy goals on raising cyber safety 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 might be beneficial. In addition, international standards can be used as a basis for establishing or demonstrating conformance to regulation, supporting interoperability and regulatory compatibility with systems in other jurisdictions.

The opportunity, and challenge, for Australian stakeholders is to effectively use the standards development process and the standards that are already developed to purchase and use consumer-grade smart devices which are cyber secure. Internationally aligned standards can help to decrease barriers to trade, ensure quality and build greater public and consumer trust in digital products and services.

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

Accordingly, SA recommends the Australian Government continue to support Australia's participation in standards setting internationally through SA's trusted and established processes.

International responsible cybersecurity standards

IT-012 is a large, joint Australian and New Zealand committee with representation across:

- User and Purchasing Bodies
- Government Organisations
- Consumer Interests
- Manufacturers' Associations
- Professional Associations
- Technical Associations
- Research and Academic Organisations
- Certification Bodies
- Regulatory and Controlling Bodies
  You can find the committee constitution here: IT-012 Information security, cybersecurity and privacy protection | Account | Salesforce.

Information on **ISO/IEC JTC 1/SC 27** here:

- ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection
- About (iso.org).
- List of published Standards: ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection
- Standards under development: ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection

Australian mirror committee for ISO/IEC JTC 1/SC 27 is **IT-012 Information security, cybersecurity and privacy protection**.

IT-012 Scope: The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy (particularly PII) aspects.

Included:

- Management of information and ICT security including the application of governance and risk principles; in particular information security management systems, security processes, and security controls and services;
- Management of personal information (also known as personally identifiable information (PII)) including the application of privacy governance and principles;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Techniques for managing the identity of people, organizations (non-person legal entities), and items of equipment and software;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; and

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

- Security evaluation criteria and methodology.

Current work:

- AS/NZS ISO/IEC 27551 Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication – we are waiting on SNZ approval. This will likely be published in January 2024 (either AS or AS/NZS).
  The committee is looking to adopt the following ISO/IEC JTC 1/SC 27 Standards/Technical Reports (identical adoptions) in the upcoming months:
- ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines
- ISO/IEC 27559:2022 Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework
- ISO/IEC 27557:2022 Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management
- ISO/IEC TR 22216:2022 Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022

  The committee will be discussing the adoption of the following ISO/IEC JTC 1/SC 27 Standards/Technical Reports in the upcoming months:

- ISO/IEC 27553-1:2022 Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 1: Local modes
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO/IEC 27556:2022 Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework
- ISO/IEC TR 5895:2022 Cybersecurity — Multi-party coordinated vulnerability disclosure and handling
- ISO/IEC 27036-2:2022 Cybersecurity — Supplier relationships — Part 2: Requirements
- ISO/IEC 27099:2022 Information technology — Public key infrastructure — Practices and policy framework
- ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model
- ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components
- ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components
- ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities
- ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements
- ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation

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

SA collaborating with ACCA to create mandatory standards

There are many factors for the regulator to consider in how they develop their policy, how far reaching it should be, what penalties should be place, how it should be enforced etc. Coming at this from a blank slate can be a significant challenge, as with many such situations, regulators often undertake consultation in order to get insights from the industry and consumers. Standards Australia engaged consistently over time through a variety of mediums. Informal and formal virtual meetings in the first instance to build rapport and generate awareness of the resources we can provide, combined with regular follow ups to reinforce the same. As things progressed, we provided a combination of written submissions and input at in person consultations. Throughout that process we conveyed the wide variety and depth of the information available in the voluntary standards, we also brought in experts involved in developing them to get our point across, and provided presentations to demonstrate the intended purpose behind each individual document within the series.

Local policy makers are often unaware of specific voluntary/ISO standards and will usually rely on local consultations to inform their decisions as they often are looking to address local issues. Even if they are aware that relevant ISO standards exist, they often do not understand the ISO ecosystem well enough to access them or may even just assume that an international is unlikely to relate to their specific market. The possibility of a modified adoption to address that for example, is not something they would consider in the first instance, our engagement with these policy makers can often be the difference in international standards being considered altogether.

Using standards to support responsible cyber security regulation including and beyond the Security of Critical Infrastructure Act 2018 (SOCI Act)

The Australian Government has a critical role increasing cyber safety and regulatory pathways for cyber security in Australia, across both consumer grade smart devices and critical infrastructure. The SOCI Act plays a significant role in strengthening Australia's critical infrastructure, standards can continue to support the foundations of reforms to SOCI. All levels of governments must carefully consider implementing relevant international standards as the basis for establishing common approaches to the regulation cyber security.

To support these considerations, SA suggests the Australian Government work with SA and industry to carefully consider how standards are to be best used for what purposes and in relation to specific public policy requirements in the SOCI Act.

Government regulators can benefit from standards that establish a solid technical base that can be used to establish policy objectives and can be used as a means of demonstrating conformance with emerging regulatory requirements. Regulation frameworks based on standards can facilitate understanding and uptake of cyber security and its vulnerabilities.

SA supports the Australian Governments ambitions to combine the relevant security obligations of the Telecommunications Act with the SOCI Act into a new TSRMP. SA can help with the modification, adoption or development of relevant standards which can aide the Australian Government's ambition to align relevant standards.