Submission to Horizon 2 of the 2023–2030 Australian Cyber Security Strategy

IEEE Members
[redacted]

Executive Summary

IEEE (Institute of Electrical and Electronics Engineers) is the world's largest technical professional association, with a significant presence in Australia. The IEEE Society on Social Implications of Technology (SSIT) Australia chapter, a community of experts on the social and ethical dimensions of technology, has prepared this submission. We commend the Australian Government's consultative approach in the development of Horizon 2 and are pleased to offer a continued and expanded perspective on the challenges and opportunities for Australia's cyber security strategy.

This submission is grounded in the expertise of a diverse range of researchers and industry professionals. We believe the success of Horizon 2 will be determined by practical implementation, regulatory coherence, and a shared national ownership of cyber resilience that extends beyond purely technical considerations. We are fully supportive of the Government's intent and stand ready to assist in the implementation of the initiatives that arise from this consultation process.

Strategic Outlook for Horizon 2

The accelerating pace of digital transformation, encompassing developments in generative AI, quantum computing, digital identity, and data brokerage, will continue to reshape Australia's cyber risk profile. These changes necessitate a proactive approach to regulation, the modernisation of our compliance infrastructure, and a greater level of coordination between policy, risk management, and business operations.

The success of Horizon 2 will be defined by its ability to translate strategic vision into tangible, effective outcomes. By focusing on practical, multi-disciplinary initiatives and fostering strong collaboration between the government, industry, and the expert community, we can collectively secure Australia's digital future. This submission is made in good faith, and we look forward to the continued consultation process.

Key Points for Consideration

- **The Need for Safety:** The strategy must address cyber threats in the physical world, which are often overshadowed by online threats. The protection of physical safety is paramount in critical sectors such as medical and transport, where a compromise of operational technology could have dire consequences. We recommend that the extensive protection of critical infrastructure currently being undertaken by the Federal government be reflected prominently in the final strategy.
- **Regional Cooperation:** Australia should leverage its existing international agreements on trade, travel, and policing to establish a baseline approach to cyber security with our regional neighbours. Initial areas for cooperation could include air traffic control and communications systems, where established safety and critical infrastructure agreements are already in place.
- **International Law and Standards:** Australia should articulate a more detailed national position on how international law applies in the cyber context, specifically by expanding its stance on sovereignty and due diligence. We also recommend that Australia continue to actively participate in the development of international standards through technology-focused standards bodies, such as the IEEE Standards Association (IEEE SA).
- **Beyond the STEM Agenda:** A large proportion of cyber attacks originate from social engineering, a discipline outside the traditional STEM fields. Therefore, the strategy should not adopt a purely STEM-centric approach. A holistic perspective must be taken, encompassing the economic, psychological, legal, and public policy aspects of cyber security.
- **Developing the Cyber Workforce:** A key challenge for Australia is the development of its cyber security workforce. We should not rely solely on professional immigration but view this as a significant opportunity to build a skilled workforce capable of providing services to our region and beyond.
- **Emerging Technologies:** The strategy should proactively consider the cyber security challenges posed by emerging technologies, including automated driving systems and social media platforms. It is imperative to promote and enforce a "security by design" philosophy from the earliest stages of technology development.

28 August 2025

To: Department of Homeland Affairs

RE: Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

The IEEE Standards Association (IEEE SA) welcomes the opportunity to provide its comments on the Australian Department of Homeland Affairs Policy Discussion Paper of Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

IEEE SA is a globally recognized standards-setting body within IEEE, the largest organization of technology professionals in the world. We develop consensus standards through an open process that engages industry and brings together a broad stakeholder community.

As stated in the draft policy discussion paper, IEEE SA recognizes that this is an important step in extending the reach of national security maturity across the country.

IEEE SA offers the following comments to the Consultation Questions

1. For the General Question on the Outlook for Horizon 2-- What trends or technology developments will shape the outlook over the next few years and what other strategic factors should the Government be exploring for cyber security under Horizon 2?

IEEE SA would like to propose the following list of technology areas that should be covered in the Horizon 2: strategy:
- Artificial Intelligence and Cloud/Data Sovereignty
- Cyber Workforce -Introducing Cyber Security at High schools as a mandatory course curriculum
- Threat Sharing Platform among organizations led by Government and Independent bodies.
- Australia to lead cyber partnerships at APAC, help set and uplift regional standards.
- Supply Chain Security - Vigilant regulation of software, hardware, and managed service supply chains is important.

We propose that Horizon 2 should also have an additional focus on these strategic factors:
- Accelerating pace of "security as a premium tier" in new and existing technologies
- Cyber Awareness, introducing Cyber Awareness and education at Primary School level as part of National curriculum
- Leading/enabling a regional CVE data feed with funding of groups such as MITRE to provide resilience against geo-political risks (i.e. March 2025 temporary funding halt in US)

2. For the Question on Shield-level focus for Horizon 2-- Shield 1: Strong businesses and citizens--What are the unique challenges that NFP entities face for cyber security compared to

the broader business sector and what interventions from government would have the most impact in the NFP sector?

IEEE SA would like to note that NFP's vary widely in their access to funding. Offering/supporting access to necessary cyber security capabilities via assistance schemes with mandatory compliance requirements to maintain access etc., might be an approach to encourage adoption and address the issue of affordable and accessible cybersecurity insurance products as smaller entities cyber insurance could be prohibitively expensive and difficult to access. Availability of regionally homed providers and/or government supported "safety net" provisions could alleviate this access barrier.

However, IEEE SA would like to note that it is important for policymakers to be aware of the evolving nature of cybersecurity, well-designed international standards could minimize disparities in how Horizon 2 strategies are deployed and used across different regions, ensuring a baseline level of technical requirements are met.

At IEEE SA, our community has developed resources and standards globally recognized in cybersecurity. The value of adhering to a standards-based approach for the Horizon 2 strategy is that in developing and deploying products and for compliance, standards can help mitigate potential risks as well as to enable compliance, and interoperability between products and within systems.

IEEE would recommend aligning technical controls with established IEEE standards that are especially relevant to addressing specific areas within the Horizon 2 proposal such as edge devices, OT/ICS systems, supply chain safety, and enterprise network protection.

The following is a partial list of IEEE Standards that are relevant for the development of the Horizon 2 cybersecurity strategy:

IEEE 1547.3™-2023, Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems provides guidelines for Cybersecurity of Distributed Energy Resources (DER) interconnection with Electric Power Systems (EPS).

IEEE 1686™-2022, IEEE Draft Standard for Intelligent Electronic Devices Cyber Security Capabilities addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an Intelligent Electronic Device (IED).

IEEE P2658™, Guide for Cybersecurity Testing in Electric Power Systems provides test guidance for cybersecurity controls used in electric power systems.

IEEE P2808™, Standard for Function Designations used in Electrical Power Systems for Cyber Services and Cybersecurity applies to the definition of function designations for cyber-related services, and cybersecurity controls and measures used to detect, identify, protect from, respond to, and recover from, security threats to electric power systems.

IEEE P2968.2™, Trial Use Recommended Practice for Decentralized Clinical Trials Threat Modeling, Cybersecurity, and Data Privacy describes a set of minimum requirements and useful considerations that can be applied to threat modeling when assessing the cybersecurity and data privacy of protocol design and technology implementation for decentralized clinical trials.

IEEE P9274.4.2™, Recommended Practice for Cybersecurity in the Implementation of the Experience Application Programming Interface (xAPI) describes the technical implementation of cybersecurity for xAPI and includes information an implementer would find useful related to matters of best practice in privacy and security, and related matters in conformance and testing.

IEEE 1686™-2022, IEEE Draft Standard for Intelligent Electronic Devices Cyber Security Capabilities addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an Intelligent Electronic Device (IED).

IEEE P2808™, Standard for Function Designations used in Electrical Power Systems for Cyber Services and Cybersecurity applies to the definition of function designations for cyber-related services, and cybersecurity controls and measures used to detect, identify, protect from, respond to, and recover from, security threats to electric power systems.

IEEE/ISO 11073-40102-2022 IEEE/ISO International Standard - Health informatics--Device interoperability Part 40102: Foundational--Cybersecurity--Capabilities for mitigation covers Personal Health Devices (PHDs) and Point-of-Care Devices (PoCDs), and establishes a security baseline of application layer cybersecurity mitigation techniques for certain use cases or for times when certain criteria are met.

IEEE 1547.3™-2023, Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems Guidelines for Cybersecurity of Distributed Energy Resources (DER) interconnection with Electric Power Systems (EPS).

IEEE P2658™, Guide for Cybersecurity Testing in Electric Power Systems Test guidance for cybersecurity controls used in electric power systems.

IEEE P2968.2™, Trial Use Recommended Practice for Decentralized Clinical Trials Threat Modeling, Cybersecurity, and Data Privacy Recommended practice describes a set of minimum requirements and useful considerations that can be applied to threat modeling when assessing the cybersecurity and data privacy of protocol design and technology implementation for decentralized clinical trials.

IEEE P9274.4.2™, Recommended Practice for Cybersecurity in the Implementation of the Experience Application Programming Interface (xAPI) Recommended practice describes the technical implementation of cybersecurity for xAPI and includes information an implementer would find useful related to matters of best practice in privacy and security, and related matters in conformance and testing.

IEEE P2887 Recommended Practice for Zero Trust Security provides security guidance for Zero Trust Security (ZTS) architectures and implementations.

IEEE 3152-2024™ Standard for Transparent Human and Machine Agency Identification defines elements to improve transparency in the identification of the agency behind media or communications, such as machine intelligence, a human being, or a combination of entities, are defined in this standard. The goal is to facilitate transparency, understanding, and trust during online, telephone, robotic, or other electronic interactions, thereby strengthening provisions for public safety and security.

IEEE 802.1AR-2018™ –Local and Metropolitan Area Networks - Secure Device Identity d mechanisms for uniquely identifying and authenticating devices using cryptographic identity—useful for ensuring trustworthy edge devices and enforcing baseline protections.

IEEE 802.1AE-2006 ™ Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security specifies how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.

IEEE 802.1X-2020 Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and that secure communication between the ports, including the media access method independent protocols that are used to discover and establish the security associations used by IEEE 802.1AE(TM) MAC Security.

IEEE 1363-2000 ™ Standard Specifications for Public-Key Cryptography specifies common public-key cryptographic techniques, including mathematical primitives for secret value (key) derivation, public-key encryption, and digital signatures, and cryptographic schemes based on those primitives. It also specifies related cryptographic parameters, public keys, and private keys.

IEEE 1363.3-2013 Standard for Identity-Based Cryptographic Techniques using Pairings Common identity-based public-key cryptographic techniques that use pairings, including mathematical primitives for secret value (key) derivation, public-key encryption, and digital signatures, as well as cryptographic schemes based on those primitives are specified in this standard. Also, related cryptographic parameters, public keys and private keys, are specified.

IEEE 1619-2025 ™ Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices specifies the XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing (XTS) cryptographic mode of operation for the Advanced Encryption Standard (AES) block cipher for logical block-oriented storage devices

IEEE 1451.0-2024M Standard for a Smart Transducer Interface for Sensors and Actuators--Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats The common functions, network services, transducer services, and Transducer Electronic Data Sheet (TEDS) formats for members of the IEEE 1451 family of standards to be interoperable in both network interface and transducer interface are provided. The common functions and characteristics that are to be performed by a network capable application processor (NCAP), which is a 1451 server, and all devices that implement the NCAP are defined. A set of network services that includes a set of commands and replies to access transducer data and TEDS data from the NCAP (1451 server) by the Internet of Things (IoT) applications (APPs) that are 1451 clients are also defined. Application programming interfaces (APIs) of network services are outlined to facilitate communications between the APPs (1451 clients) and NCAPs. Furthermore, the common functions and characteristics that are to be performed by a transducer interface module (TIM) and all devices that implement the TIM are discussed. A set of transducer services that includes a set of commands and replies to facilitate the setup and control of the TIM, as well as reading and writing the data used by the NCAP, are outlined. APIs of transducer services are also discussed to facilitate communications between the NCAPs and TIMs. Finally, the formats for a TEDS and methods to access the TEDS are specified, along with the common functions and characteristics that are to be performed by an APP and all devices that implement the APP. Additional Open Source content available here: https://opensource.ieee.org/1451/1451.0-schema/

IEEE 1849-2023 ™ Standard for eXtensible Event Stream (XES) for Achieving Interoperability in Event Logs and Event Streams A grammar for a tag-based language whose aim is to provide designers of information systems with a unified and extensible methodology for capturing systems' behaviors by means of event logs and event streams is defined in the XES standard. An "XML Schema" describing the structure of an XES event log/stream and an "XML Schema" describing the structure of an extension of such a log/stream are included in this standard. Moreover, a basic collection of so-called "XES extension" prototypes that provide semantics to certain attributes as recorded in the event log/stream is included in this standard.

IEEE SA's portfolio of cybersecurity standards and programs can be found here: https://standards.ieee.org/initiatives/cybersecurity-standards-projects-2/

We would look forward to further discussions with the Department of Homeland Affairs on developing the Horizon 2 Australian Cyber Security Strategy.

If you have questions, please do not hesitate to contact [redacted]