IGEA

interactive games & entertainment association

Submission to Cyber and Infrastructure Security Centre, Department of Home Affairs

Response to Exposure Draft of the Cyber Security (Security Standards for Smart Devices) Rules 2024

February 2025

IGEA acknowledges and pays respect to the past and present Traditional Custodians and Elders of this land and the continuation of cultural, spiritual and educational practices of Aboriginal and Torres Strait Islander peoples. We would like to extend our acknowledgments to the indigenous people from countries overseas and recognise their strength, wisdom and creativity.

1. Introduction

The Interactive Games & Entertainment Association (IGEA) welcomes the opportunity to provide a submission to the consultation on the exposure draft of the Cyber Security (Security Standards for Smart Devices) Rules 2024 (and accompanying explanatory document), led by the Cyber and Infrastructure Security Centre (within the Department of Home Affairs).

1.1 About IGEA

IGEA is the industry association representing and advocating for the video games industry in Australia, including the developers, publishers and distributors of video games, as well as the makers of the most popular game platforms, consoles and devices. IGEA has over a hundred members, from emerging independent studios to some of the largest technology companies in the world. Of most relevance to our engagement on the topic of cyber security for smart devices, our members include the manufacturers of devices for the playing of video games (video game consoles).

Amongst our various activities, IGEA also organises the annual Games Connect Asia Pacific conference for Australian game developers and the Australian Game Developer Awards that celebrate the best Australian-made games each year.

Video games are a beloved Australian activity and significantly benefit Australian game players, the wider community, and the economy. Video game developers and publishers are the innovators, creators and business leaders reimagining entertainment and transforming how we learn and play. Over 80% of Australians play games, with most Australian households having a device for playing video games, mainly for enjoyment and relaxation, and games are increasingly being used for serious and educational purposes, including by governments.[1] Video games provide a digital outlet for Australian art, culture, stories and voices, and Australian-made video games are among Australia's most successful and valuable cultural exports. Our medium also brings kids into Science, Technology, Engineering, the Arts and Mathematics (STEAM) and helps them build technology skills to feed Australia's workforce needs.

In supporting local content, the video games industry is a major contributor to the Australian digital economy. According to our data, video games are worth around $4.4 billion annually in Australia,[2] while Australian-made games brought in $339.1 million in largely export revenue last financial year.[3] Moreover, because the video games industry uniquely sits at the intersection of entertainment, the arts and technology, video game companies hire a wide range of artistic, technical and professional roles and are thus a wellspring of high-quality sustainable careers, and are an engine for growth in the

[1] IGEA, 'Australia Plays' (August 2023), https://igea.net/2023/08/australia-plays-2023/.

[2] IGEA, '2023 Australian video game consumer sales continue stable growth' (Media Release, June 2024), https://igea.net/2024/06/2023-avgcs/.

[3] IGEA, 'Australian video game development industry stays steady, generating $339.1 million for the economy' (Media Release, December 2024), https://igea.net/2024/12/australian-video-game-development-industry-stays-steady-generating-339-1-million-for-the-economy/.

Australian national economy. Indeed, Australian game developers are internationally renowned, and ours has the potential to be one of Australia's most important future growth industries and an integral component of the government's vision for Australia to be a top 10 digital economy and society by 2030.

1.2 Overview of submission

With respect to the exposure draft rules for smart device security standards in Australia, any proposed rules should be regulatory coherent with similar overseas legislation (including standards), as we stated in our previous submission.[4] We understand that there is an intention for coherence with other regimes, such as the UK *Product Safety and Telecommunications Infrastructure Act 2022* (UK's approach), especially around the terminology 'relevant connectable products' and requirements for statements of compliance.[5] The objective of this is to "reduce the burden on industry operating across jurisdictions and ensure Australians purchasing smart devices are protected to the same extent as international counterparts".[6]

For this to be coherent, we should avoid a situation in which Australian legislation and regulation are significantly different and more onerous than other jurisdictions. For example, voluntary flexible measures from other jurisdictions should neither be adopted nor prescribed as mandatory requirements in Australia.

The regulatory compliance processes should be streamlined as much as possible to make them practically workable and administratively cost-efficient. Further, any proposed reforms need to be rigorously scrutinised against a proper cost-benefit assessment.

As a matter of good regulatory practice and policy design, any regulatory measure should be well-defined, reasonable and clearly scoped, provide sufficient flexibility that is future-proofed for evolving technologies, and be supplemented by relevant industry guidance to enable sufficient regulatory clarity and certainty.

For the remainder of our submission, we will focus on the regulatory compliance and administrative aspects of implementing smart device security standards, as proposed in the exposure draft rules.

Below is a summary of our recommendations on the exposure draft rules:

Topic	**IGEA's recommendations**
Statements of compliance	We would like to confirm with the Government whether the manufacturer or supplier will only be required to make a self-declaration of conformance and can be accessed online by auditors as required. We consider this to be the

[4] IGEA submission to PJCIS inquiry, https://www.aph.gov.au/DocumentStore.ashx?id=d90f15ac-2d00-44cf-811f-657561e34bc4&subId=768788.

[5] Explanatory Memorandum to the Cyber Security Bill, pp. 3-4, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r7250_ems_2474a1f7-f1f0-4895-9113-3b8532da3377/upload_pdf/JC014269.pdf;fileType=application%2Fpdf.

[6] Ibid, p. 3.

Topic	IGEA's recommendations
	most administratively efficient approach that still meets the Government's requirements.
Lessons learnt from the UK's approach	Explore lessons learnt from the UK's approach to implementing security standards for smart devices, leveraging on insights from UK-regulated entities, and implement improvements for the Australian approach.

2. Scope of smart devices under the standard

The explanatory document to the exposure draft rules identifies smart devices that will be covered in the scope of the security standard to be defined as 'relevant connectable product', in accordance with section 13 of the *Cyber Security Act 2024* (Cth) – we understand that such a device would be "reasonably acquired by a consumer per Australian Consumer Law". We further understand that there is an intention for the scope of smart devices to be similarly defined, captured and exempted as those under the UK's approach.

In principle, we do not object to the scope of devices proposed to be captured and exempted, especially when applying regulatory coherence with overseas approaches. In this regard, we understand that the Government has chosen to implement domestic requirements aligned with those from overseas, such as in the UK. This is intended to acknowledge that Australia is a net importer of consumer goods (including smart devices), does not intend to create unnecessary technical barriers to trade,[7] and therefore expects that devices imported from overseas should already comply with cyber security requirements. Further, if properly implemented, this will ensure genuine regulatory coherence is achieved in practice, and reducing the regulatory burden on industry operating across jurisdictions subject to the same level of protections, by recognising acceptable overseas security requirements.

3. Statements of compliance

According to the Explanatory Memorandum to the Cyber Security Bill 2024, responsible entities must provide a statement of compliance for their smart devices supplied to the Australian market. We understand that details within the statement of compliance has been based on the UK's approach.

In the first instance, we would like to confirm with the Government whether the manufacturer or supplier will only be required to make a self-declaration of conformance. Such a declaration will not need to be physically published, and can be accessed online by relevant auditors as required. This approach will be more administratively efficient while still meeting the government's intended policy. In particular, it will help companies streamline the process, minimising the regulatory costs associated with revising product manuals for the smaller Australian market. Further, not requiring the need for physical documentation avoids information that may become outdated over time for remaining

[7] For instance, see: https://www.dfat.gov.au/trade/organisations/wto/technical-barriers-to-trade-tbt.

stocks, therefore providing the most updated information online, and also aligns with the Australian Government's environmental sustainability packaging agenda.[8] (We discuss further below about lessons learnt from industry's experience with the UK's approach on statements of compliance that can be improved upon in the Australian context.) However, should the Government consider implementing other approaches to statements of compliance, it needs to be as administratively efficient as possible.

Recommendation: We would like to confirm with the Government whether the manufacturer or supplier will only be required to make a self-declaration of conformance and can be accessed online by auditors as required. We consider this to be the most administratively efficient approach that still meets the Government's requirements.

4. Lessons learnt from the UK's approach

Given that Australia is drawing largely from the UK's approach, it would be prudent to improve upon the lessons learnt from the UK's implementation. The general feedback that we have received on significant issues with the UK's approach include:

- The implementation of the new UK regulations was rushed in a very tight timeframe. In particular, any 'supply' of regulated products after a certain date meant that existing stock in the market was affected.
- The UK regulator was very inflexible towards how aspects of the requirements were implemented by regulated entities, such as in relation to information on the defined support period for security updates that are required to be published.

Specifically related to statements of compliance, as discussed above, there are indeed improvements that can be made in the Australian context. We understand that manufacturers in the UK are already obligated to make information available online and direct consumers to a webpage containing information on the support periods for their devices. It would be pertinent to utilise existing pages for the purpose of demonstrating compliance with the Australian regime by directing consumers to a page which already exists to reduce the burden required to add additional documentation for products destined for Australia. This would also allow for the page to be updated periodically without having to then make changes to physical documentation.

However, a key problem with the UK's approach relates to retailers who have had to reach out to a high number of manufacturers for confirmation that physical documentation are up-to-date to ensure that the statement of compliance obligation has been fulfilled. This reinforces a further reason why a 'digital first' approach should apply for demonstrating compliance.

[8] For example, the major video game console manufacturers are signatories to the Australian Packaging Covenant Organisation, https://apco.org.au/.

Recommendation: Explore lessons learnt from the UK's approach to implementing security standards for smart devices, leveraging on insights from UK-regulated entities, and implement improvements for the Australian approach.

Thank you for allowing IGEA to contribute to this consultation. For more information on any issues raised in this submission, please contact us at policy@igea.net.