

**International Social Games Association –
CONFIDENTIAL AND PRIVILEGED**

January 19th, 2024

To: The Office of the eSafety Commissioner

Email: submissions@esafety.gov.au

**Submission on the Draft Online Safety (Relevant Electronic Services –
Class 1A and 1B Material) Industry Standard 2024**

Introduction

The International Social Games Association (ISGA) acknowledges the Office of the eSafety Commissioner (‘eSafety’) for inviting submissions on the Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024 (‘RES Standards’). ISGA welcomes the opportunity to provide feedback as Australia continues to play a leading role in online safety policy making.

ISGA is an international non-profit industry association established in 2013 to develop and communicate global best practices in social games. ISGA represents social (or mobile) games businesses, including Greentube, IGT, HUUUGE Games, Pixel United, Playstudios, Playtika, and Zynga. Together, we promote player education through our Smart Mobile Games website¹, developed with leading digital safety organisations, clinical psychologists, and games researchers.

ISGA has a regularly updated set of Best Practices Principles² (‘Principles’) based on the core values of online safety, accountability, and transparency. ISGA is proud to be taking the lead in responsible standards for the sector and we are pleased that our Principles have been endorsed by an Australian Parliamentary committee:

‘The International Social Games Association (ISGA), the global industry body for social games companies (including simulated gambling games) specifically discourages its members from promoting simulated gambling products to users under the age of 18 years. The ISGA also provides an online resource called ‘Smart Mobile Gamers’ to give guidance, tips, and advice on topics such as parental controls and managing in-game spending. It has partnered with digital safety organisations and experts to create this website.’³

Around 55% of video games played by Australians are enjoyed on mobile devices. The mobile games market is a vibrant, but complex, global consumer market. Our organisation therefore has a material interest in ensuring effective policy making in this area in all major jurisdictions, including Australia.

Since we were established in 2013, ISGA has proactively engaged with pivotal issues in the digital world, such as online safety, consumer protection, and privacy by design. Most recently, we supported and assisted the Federal Government in prioritising updates to the National

¹ www.smartmobilegamers.org

² <https://www.i-sga.org/best-practice-v5>

³

https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Online_verification/Government_Response

**International Social Games Association –
CONFIDENTIAL AND PRIVILEGED**

Classification Scheme, which seek to protect those most vulnerable in our community, including children.

Executive Summary

ISGA welcomes the modernisation of Australia’s Online Safety Framework and broadly supports commitments to a fit-for-purpose Online Safety Act that makes online services more accountable for the safety of their users. We are encouraged by the outcomes- and risk-based approach to the RES Standards, whereby proposed requirements aim to be proportionate to the risk a service presents in respect of class 1A and 1B material. It is vital that online services take effective steps in addressing harms caused by the dissemination of child sexual exploitation material and other forms of illegal content. These steps must be taken in a proactive and proportionate manner, in consideration of a user’s right to privacy and freedom of expression. We also appreciate eSafety’s efforts in aligning with other regulatory bodies, both domestically and internationally⁴, to provide certainty, consistency, and uniformity. ISGA respectfully proposes the following recommendations:

- The RES Standards should reflect the position paper and make clear, where appropriate, that they apply only to content imported into a game environment via the game’s interactive tools which is separate to the game itself and which is likely to be classified as class 1 or class 2 material.
- The full content of Annexure A (Guidance on Classification Process), from the Head Terms of the Consolidated Industry Codes of Practice for the Online Industry (Class 1A and 1B Material) should be adopted into the RES Standards to provide coherence with the National Classification Scheme.
- We note the desired policy intention to regulate services in a manner proportional to the risk of Class 1A and 1B materials. As a result, where a gaming service is pre-assessed to be one with communications functionality, the relevant obligations should be according to the level of risk on the service, as opposed to automatically applying unintended onerous and costly obligations that are akin to a Tier 1 Relevant Electronic Service.
- Section 22 of the RES Standards, as well as the discussion paper, should be amended:
 - The discussion paper should amend its justification for the inclusion of games with communications functionality to accurately reflect what is in scope of the draft RES Standards and that existing research is limited.
- ISGA recommends eSafety amends the RES Standards to extend the ‘technical feasibility’ exemption to Section 27 at a minimum.
- The definition of large services should be amended to reflect a consistent international approach to online safety that provides clarity to online services.
- We recommend removing Section 37 of the RES Standards, as Section 38 sufficiently empowers the Commissioner to require compliance reports.

Feedback on the RES Standards

1. Scope – ‘content that has not yet been classified’

⁴ As is demonstrated by the eSafety Commissioner’s role as Chair of the Global Online Safety Regulators Network

**International Social Games Association –
CONFIDENTIAL AND PRIVILEGED**

The Online Safety Act takes a novel approach to the classification of user-generated online content by classifying such content in a way which corresponds to the manner in which films are classified under the National Classification Scheme. As such, our interpretation is that eSafety views online content as a standalone category of material. Therefore, the difference between user-generated online content and commercially produced material should be reflected and made explicit in the RES Standards.

eSafety's Position Paper on the 'Development of industry codes' ('position paper') clarifies the scope for Relevant Electronic Services (RES), which includes online games where end-users can play against each other. Furthermore, the 'codes will not apply to game content which has been classified in Australia. However, the codes will apply to content imported into a game environment via the game's interactive tools which is separate to the game itself and which is likely to be classified as class 1 or class 2 material'⁵. This clarification provides certainty for online games to be able to take effective steps in managing and mitigating such content. While eSafety has a leadership role in online safety, the work of other regulatory bodies, such as the Classification Board, to keep Australians safe online must be recognised.

Recommendations

- The RES Standards should reflect the position paper and make clear, where appropriate, that they apply only to content imported into a game environment via the game's interactive tools which is separate to the game itself and which is likely to be classified as class 1 or class 2 material.
- The full content of Annexure A (Guidance on Classification Process), from the Head Terms of the Consolidated Industry Codes of Practice for the Online Industry (Class 1A and 1B Material) should be adopted into the RES Standards to ensure coherence with the National Classification Scheme.

2. Measures should be reasonable and proportionate, based on an assessment of risk

ISGA supports eSafety's position that risk assessments are an important way to reduce the risks of class 1A and 1B material being generated, posted, stored, or distributed⁶. However, we strongly disagree that 'games with communications functionality' should be deemed pre-assessed as high-risk services in all instances and therefore 'exempt' from risk assessment requirements.

According to the position paper, measures should be reasonable and proportionate, based on an assessment of the risk an industry participant's services or devices present in respect of class 1 and class 2 material.⁷ This rationale is reflected in the EU and the UK⁸. To the contrary, by defining games with communications functionality as pre-assessed, the majority of online games will be subject to minimum compliance measures akin to the highest risk Tier 1 services regardless of their size.

⁵ <https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf> – p.33

⁶ <https://www.esafety.gov.au/sites/default/files/2023-11/Discussion-Paper-draft-Online-Safety-Standards-%28Class-1A-and-1B%29.pdf> – p.10

⁷ <https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf> p.6

⁸ Ofcom's draft guidance on illegal harms categorises services according to size and level of risk.

**International Social Games Association –
CONFIDENTIAL AND PRIVILEGED**

The justification for this pre-assessment appears to be based on: a) research which indicates that the communications features in gaming services are used to approach children and coerce them into creating child sexual abuse material, and b) research that ‘suggests’ that gaming services could be used to circulate pro-terror material even though the research referenced appears to point mainly towards games-adjacent communications platforms, like Discord and Twitch, and not to the functionality enabled within online gaming services themselves. It appears that the evidence of the actual use of online gaming services for such illicit purposes is very limited and that ‘there are certain key questions whose answers remain elusive’⁹. The presence of potential harms on games-adjacent communications platforms should have no bearing on the risk profile of online gaming services.

Similarly, it should be clarified within the RES Standards that third party communications functionality that is enabled or linked to from within an online gaming service, but which is external to the online gaming service itself (for instance, the voice chat functionality provided by many of the digital distribution platforms and devices through which online gaming services are played), does not result in the online gaming service being deemed to have communications functionality as a result of allowing players to avail themselves of such third party communications functionality.

We believe that assigning games with communications functionality as ‘pre-assessed’ is contrary to the policy intention of the RES Standards, whereby services are given the flexibility to implement effective, proportionate measures based on an accurate assessment of risk. The discussion paper clarifies that eSafety ‘considers it appropriate to limit [Section 23] to large relevant electronic services, reflecting both the greater risk of dissemination on services with a large number of end-users’. Size and risk of dissemination are two of a multitude of factors that must be considered before it can be concluded that a service is subject to similar obligations of the Tier 1 services merely due to the communications functionality component.

Recommendations

- Where a gaming service is pre-assessed to be one with communications functionality, the relevant obligations should be according to the level of risk on the service, as opposed to automatically applying unintended, onerous, and costly obligations that are akin to a Tier 1 Relevant Electronic Service.
- Section 22 of the RES Standards, as well as the discussion paper, should be amended:
 - The discussion paper should amend its justification for the inclusion of games with communications functionality to accurately reflect what is in scope of the RES Standards and that existing research is limited.

3. Technical feasibility

eSafety sets out in Section 7 of the RES Standards the matters to be considered while determining technical feasibility include ‘expected financial cost to the service of taking the action’ and ‘whether it is reasonable to expect the service to incur that cost, having regard to the level of the risk of the online safety of end-users in Australia of not taking the action’. This is a crucial consideration that acknowledges that it is appropriate to provide flexibility to

⁹ https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

**International Social Games Association –
CONFIDENTIAL AND PRIVILEGED**

services to take alternative action where it is technically infeasible to comply. Accordingly, ISGA respectfully questions why the technical feasibility exemption is not applied throughout the document. We acknowledge that this is an intended solution for end-to-end encrypted services. However, a reasonable regard to make an argument for cost and risk would enable services to introduce effective measures as per the policy intention of eSafety.

For instance, games with communications functionality are subject to providing mechanisms for end-users and account holders to report, and make complaints about, material accessible through relevant electronic services. Section 27(3) explains that such a tool, process or technology must be available ‘in service’, that is, not on a separate webpage. This may not be technically feasible for an online game, operating on a mobile device, to execute, in a way that is not detrimental to the user experience or does not result in a disproportionately high burden of cost. Consumers are used to accessing support and reporting functionality through dedicated customer support websites that are external to the online gaming service they are playing. Such websites typically support the much more limited native customer support and reporting functionality that is available in-game and are not encumbered by the technical limitations presented in-game.

Recommendations

- ISGA recommends eSafety amends the RES Standards to extend the ‘technical feasibility’ exemption to Section 27 at a minimum, so that services can provide effective, tailored solutions.

4. A consistent international approach to online safety

Australia’s Online Safety Act is a world-first landmark framework that has been followed in the EU with the Digital Services Act, and recently in the UK, with the Online Safety Act. While all follow the same broad aims, to hold online services accountable for the safety of their users, the requirements for each vary, creating difficulties for in-scope services to operationalise compliance. Uniformity will be an extremely effective tool and we acknowledge the important work of eSafety in leading the way in sharing best practices.

Nonetheless, under section 23 of the RES Standards, services with more than 1 million monthly active users in Australia are defined as large relevant electronic services. Comparatively, Ofcom defines large services as those with an average monthly userbase approximately equivalent to 10% of the UK population. This reflects the EU’s Digital Services Act and its designation of 10% of the EU’s population as the threshold by which an online platform becomes a Very Large Online Platform. ISGA believes eSafety’s definition of large services should be amended to align internationally to ease barriers to compliance.

Moreover, ISGA would appreciate alignment in terms of compliance reports. Sections 37 and 38 compel in-scope services to provide an annual compliance report, as well as an added obligation to provide a compliance report under notice from the Commissioner. This creates a compliance obligation that, if replicated across jurisdictions, would incur disproportionately burdensome costs. Not only should these sections be amended to build upon appropriate safeguards that promote due process, transparency, confidentiality, and privacy, eSafety should also consider the removal of Section 37 completely, given that section 38 empowers the Commissioner to require compliance reports more generally.

**International Social Games Association –
CONFIDENTIAL AND PRIVILEGED**

Recommendations

- The definition of large services should be amended to reflect a consistent international approach to online safety that provides clarity to online services.
- We recommend removing Section 37 of the RES Standards, as Section 38 sufficiently empowers the Commissioner to require compliance reports.

Conclusion

ISGA appreciates the opportunity to contribute to this important consultation and would be pleased to provide further elaboration or information on this submission.

Luc Delany
CEO, International Social Games Association

