IGEA

interactive games & entertainment association

Submission to the eSafety Commissioner

Response to Draft Relevant Electronic Services Standard

January 2024

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 & Overview

The Interactive Games & Entertainment Association (IGEA) welcomes the opportunity to provide a submission to the eSafety Commissioner (eSafety), focused on its consultation of the Draft Relevant Electronic Services (RES) Standard for Class 1A and 1B material.

This consultation follows eSafety's decision to decline the registration of the Draft RES Code and the Draft Designated Internet Services (DIS) Code developed by industry. eSafety determined that these Codes did not meet the statutory requirements for registration because they "did not contain appropriate community safeguards for users in Australia".[1] At the time, gaming services were not explicitly cited as the reason for eSafety's rejection of these Codes.[2] Moving from the rejected Codes, eSafety decided to develop and consult on the two Draft RES and DIS Standards.

The Draft RES Standard covers a wide range of services that enable end-users to communicate with each other online. Our submission focuses on those services that enable end-users to play online games with each other.

Therefore, our submission provides preliminary views regarding certain aspects of the Draft RES Standard only, as we consider this more relevant to the video games sector. This is on the basis that gaming services have been explicitly defined in the Standard and where the predominant functionality of the service appears to be more closely aligned with the Draft RES Standard than with the Draft DIS Standard. Should eSafety consider the DIS Standard also to be applicable to the video games sector, we would welcome eSafety's guidance.

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 gaming platforms, consoles and devices.

IGEA also organises the annual Games Connect Asia Pacific (GCAP) conference for Australian game developers and the Australian Game Developer Awards (AGDAs) that celebrate the best Australian-made games each year. IGEA has over a hundred members, from emerging independent studios to some of the largest technology companies in the world.

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. Two in three Australians play games, mainly for enjoyment and relaxation, and games are increasingly being used for serious and educational purposes, including by governments. Video games provide a digital outlet for Australian art, culture, stories and voices, and Australian-made video games are among

[1] See: https://www.esafety.gov.au/industry/codes.

[2] eSafety Summary of Reasons – Relevant Electronic Services Code.

Australia's most successful and valuable cultural exports. Our medium also brings kids into STEM and helps them build technology skills that will feed Australia's workforce needs.

In supporting local content, the video game industry is a major contributor to the Australian digital economy. According to our data, video games are worth around $4.21 billion annually in Australia,[3] while Australian-made games brought in $345.5 million in largely export revenue last year.[4] Moreover, because the video game sector 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 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 20 digital economy and society by 2030.

1.2 Overview

Overall, we support the intention behind the Draft RES Standard to provide appropriate community safeguards for users in Australia. Over the last several years, IGEA and its members have been heavily engaged in and contributed to the development of the various industry online safety codes that were registered by eSafety (including for app distribution services and equipment), as well as the Draft RES Code that was declined for registration by eSafety.

Beyond the Australian industry's online safety codes, the video game industry takes consumer protection extremely seriously, offering high levels of safeguards so players and parents can enjoy video games fun and responsibly. The industry adheres to strict domestic and international data and consumer protection laws, supplemented with an age-appropriate video game content labelling scheme, along with other measures. The industry also leads in empowering players and parents with easy-to-use tools, including for managing playtime, spending, online privacy, online gameplay, and access to age-appropriate games. The industry's serious commitment and responsibility to these protections are built around global industry best practices.

As a matter of good regulatory practice and policy design, any regulatory measure (such as codes and standards) 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.

We firmly believe there would be significant benefit in providing further clarity through relevant guidance and other explanatory material to support the Draft RES Standard – we understand that eSafety intentionally omitted such guidance from this consultation stage.

---

[3] 'Australians subscribe to video game growth' (IGEA Media Release, 8 June 2023).

[4] 'Aussie game developers pull in $345.5 million for the local economy' (IGEA Media Release, 18 December 2023).

However, in the absence of draft guidance material, providing substantive comments on the Draft RES Standard has been challenging, especially as they relate to the rationale and scope behind the drafting of specific provisions. Moreover, with further clarity, this will assist in informing impacted stakeholders regarding their potential regulatory obligations and costs arising from implementing the Standards in practice. Therefore, we strongly recommend that eSafety undertakes further consultation on the draft guidance material for the Draft RES Standard.

For example, the Draft RES Standard introduces fundamental changes to the definitions of gaming services, introducing the term "primary functionality" as a modifier in the definitions of gaming services with communications functionality and those with limited communications functionality. The original definitions in the Draft RES Code did not include this modifier. As discussed below, the manner in which the phrase "primary functionality" is incorporated into the definitions creates ambiguity as to the scope of the definitions and poses significant challenges for service providers to interpret and implement the Standard. There has also been no clear explanation for these changes, noting eSafety's rejection of the Draft RES Code did not explicitly cite gaming services as the reason for rejecting the Code, leaving the justification for the altered definitions unclear.

Below is a summary of our recommendations to this consultation.

Topic	**Discussion Paper question**	**Recommendations**
Definitions for gaming services with communications functionality, and gaming services with limited communications functionality	-	To provide greater clarity, while still addressing the policy intention, we propose an amendment to the definition of "a gaming service with limited communications functionality" (as was clearer in the Draft RES Code submitted for registration) to better enable a service provider to distinguish whether it falls under either a gaming service with communications functionality or limited communications functionality, and to ensure that there are no gaps between the two definitions of gaming services, i.e. to ensure clarity that a gaming service falls within one definition or the other. This could be amended along the following lines: ***gaming service with limited communications functionality*** *means a relevant electronic service, other than a closed communication relevant electronic service, the primary functionality of which is to enable end-users in Australia to play online games with other end-users without the primary functionality of the service being to enable the sharing of user-*

Topic	Discussion Paper question	Recommendations
		generated URLs, hyper-linked text, images or videos between end-users (other than material of a kind referred to in paragraph (e) of the definition of gaming service with communications functionality in this subsection). We would welcome the opportunity to discuss further with eSafety to understand the intent underlying the revised definitions for gaming services with communications functionality and those with limited functionality. This will enable the opportunity to co-develop workable solutions that clarify the definitions accordingly, as recommended above.
Obligations for gaming services with communications functionality	-	Where a gaming service meets the definition of a gaming service with communications functionality, the service provider should be given the choice to undertake a risk assessment, as a rebuttable assumption to prove that they have a lower level of risk (and therefore subject to obligations according to their actual level of risk). Otherwise, they would be subject to the default obligations for gaming services with communications functionality.
Risk assessments	1	The appropriateness and relevance of the risk assessment requirements is contingent on further clarification of the definitions for gaming services with communications functionality, and gaming services with limited communications functionality. Section 8(5) should be amended so that a RES, which is not required to undertake an initial risk assessment, should be exempted from risk assessment requirements (similar to the services listed under section 8(6)) if there are material changes to the service.
Policy considerations	2	Addressing the matters raised in our submission should contribute to reflecting eSafety's policy considerations in setting out proposed obligations in the RES Standard. In its current form, the requirements do not strike the

Topic	Discussion Paper question	Recommendations
		appropriate balance between flexibility and enforceability, not risk neutral, and not practical with respect to online gaming services.
Applicability of the RES Standard	3	We are of the view that the RES Standard is the standard applicable to online video games and that no other code or standard applies to online games. Should eSafety determine otherwise, we would welcome guidance.
Alignment with the National Classifications Scheme	-	As a matter of good regulatory practice, 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 Class 1B Material), should be adopted in the Draft RES Standard to ensure regulatory coherence with the National Classifications Scheme and consistent with the Codes already registered by eSafety.
Encryption	4, 6	Section 7 of the Draft RES Standard should be amended to reflect eSafety's intention that encryption will be protected, along with further guidance. Section 6.1 of the Code's Head Terms should be applied to reflect a broader set of principles that preserve security of online services.
Pro-terror material (PTM)	4, 6	Rather than placing the responsibility solely on the service provider, eSafety should give further direction as to how PTM is determined, the relevant jurisdiction that decides on whether it is PTM, and the role of law enforcement agencies in assessing PTM. This is particularly given the nuance required to appropriately assess such material, which has been strongly exemplified with the current conflict in the Middle East. For example, the definition proposed in the rejected Draft RES Code had the condition that PTM means material that is Refused Classification (RC) or would be RC if assessed for classification by the Australian Classification Board.

Topic	Discussion Paper question	Recommendations
Disrupting and deterring CSAM and PTM	4, 6	Section 22 requirements for disrupting and deterring CSAM and PTM need further clarification, especially in the context of video games. With respect to the reference to "behavioural signals and patterns associated with CSAM and PTM", consideration should be given to either deleting or significantly redrafting this requirement, as it is currently vague in meaning and relevance.
Examples of industry practices	5, 7	The video games industry takes online safety extremely seriously and follows global industry best practices in implementing community protections. IGEA would welcome the opportunity to share with eSafety activities that support eSafety's objectives.
Development programs	8	eSafety should give further thought on the rationale of when a service provider should be subject to an investment obligation for development programs – a proportionate approach would be based on the level of risk of the service, as opposed to arbitrary definitions and thresholds. The reference to "synthetic material generated by AI" should be deleted under section 23, as it is undefined and unclear.
Appropriate action	9, 10	To provide more clarity, the Draft RES Standard should reinstate what would constitute "appropriate action" from the Draft RES Code.
Notifying new features	-	The requirement for notifying new features or functions under section 35 should be considered redundant and removed, as it is already covered by section 19 in the Draft RES Standard.
Reporting obligations to eSafety	-	The requirement for proactive annual compliance reports from service providers under section 37 should be removed, as section 38 empowers the Commissioner to require compliance reports more generally. Where specific requirements under section 37

Topic	Discussion Paper question	Recommendations
		is practicable and achievable, in consultation with relevant service providers, these could be incorporated into section 38 reporting requirements. The reporting obligations in the Draft RES Standard should be built upon appropriate safeguards that promote due process, transparency, confidentiality, and privacy.
Compliance costs	11	For a proper compliance costs assessment, additional clarification will be required regarding the operation of certain proposed new provisions in the Draft RES Standard such as through guidance material that has been omitted from consultation at this stage. We strongly recommend that eSafety undertakes further consultation on the associated draft guidance material for the Draft Standard.

2. Categories for gaming services

2.1 Definitions for gaming services with communications functionality and gaming services with limited communications functionality

For the purposes of our submission, we are particularly concerned with the applicability of the Standards insofar as they relate to online video games services.

As with the Code, the proposed Standard establishes two categories of video game services: those with communications functionality and those with limited communications functionality. A fundamental question relates to the definitions for "a gaming service with communications functionality", and "a gaming service with limited communications functionality" under section 6 of the Draft RES Standard. We note that changes have been made to the definitions from the previously rejected Draft RES Code to the latest Draft RES Standard, and we seek further clarification and propose amendments to address our concerns.

Under the previous Draft RES Code, the following definitions were provided:

> **gaming service with communications functionality** means a relevant electronic service that:
> (a) is not a closed communication relevant electronic service or gaming service with limited communications functionality;
> (b) enables Australian end-users to play online games with other end-users; and

(c) enables the sharing of the following types of user-generated material between end-users:
  (i) URLs or hyper-linked text;
  (ii) images; and/or
  (iii) videos,
  but
(d) excludes a service that limits the sharing of user-generated material between end-users to any or all of the following:
  (i) in-game images or footage;
  (ii) user-generated designs (such as environments and artwork);
  (iii) virtual objects or maps;
  (iv) pre-selected messages;
  (v) non-hyper-linked text that is subject to automated filtering technology; or
  (vi) ephemeral voice interactions.

gaming service with limited communications functionality means a relevant electronic service that:
(a) is not a closed communication relevant electronic service;
(b) enables Australian end-users to play online games with other end-users; and
(c) does not enable the sharing of user-generated material between end-users referred to under (c) of the definition of **gaming service with communications functionality** above, other than the type of content listed under (d) of that definition.

Under the Draft RES Standard:

gaming service with communications functionality means a relevant electronic service the primary functionality of which is:
(a) to enable end-users in Australia to play online games with other end-users; and
(b) to enable sharing of user-generated URLs, hyper-linked text, images or videos between end-users;
but does not include
(c) a closed communication relevant electronic service; or
(d) a gaming service with limited communications functionality; or
(e) a service that limits the sharing of user-generated material between end-users to any or all of the following:
  (i) in-game images or footage;
  (ii) user-generated designs (such as environments and artwork);
  (iii) virtual objects or maps;
  (iv) pre-selected messages;
  (v) non-hyper-linked text that is subject to automated filtering technology; or
  (vi) ephemeral voice interactions.

gaming service with limited communications functionality means a relevant electronic service, other than a closed communication relevant electronic service, the primary functionality of which is to enable end-users in Australia to play online games with other end-users without enabling the sharing of user-generated URLs, hyper-linked text, images or videos between end-users (other than material of a kind referred to in paragraph (e) of the definition of gaming service with communications functionality in this subsection).

In reviewing the definitions, the original version in the Draft RES Code made it clear that there were only two mutually exclusive categories of gaming services, and the definitions of each made it straightforward to distinguish whether a gaming service was categorised as one with communications functionality versus one with limited communications functionality. Specifically, any game that allows online gameplay and enables sharing of certain user-generated content was considered a gaming service with communications

functionality, and any game that allows online gameplay but does not enable sharing that sort of user-generated content was considered a gaming service with limited communications functionality.

With the introduction of the term "primary functionality" in the gaming service definitions in the Draft RES Standard, it could be interpreted that this fundamentally changes the definitions from the original meaning in the Draft RES Code. There is no clear explanation for these definitional changes. For example, in reviewing eSafety's decision to decline registration of the Draft RES Code, gaming services were not explicitly identified as the reason for rejecting the Code that would warrant changes in their definitions in the Standard.

Without clarification behind the introduction of this term, there is a potential grey area for interpretation of the definitions for gaming services, which may not fall under either definition. In such a scenario, it is unclear what specific compliance requirements would apply and whether the service provider would be required to undertake a risk assessment, which could be an onerous undertaking and contrary to the purpose of providing specific definitions for video game services and linking those definitions to specific compliance requirements.

In particular, it needs to be clarified which definition would cover a game that allows online gameplay with other users and enables some sharing of the sort of user-generated content identified in the description but whose primary functionality is not the sharing of that user-generated content. Under the new definition in the Draft RES Standard, a gaming service would only be one with communications functionality if the primary purpose of the service is *both* to enable gameplay *and* to enable the sharing of user-generated material. Alternatively, a gaming service that enables the sharing of user-generated material would not be "a gaming service with communications functionality" unless the game's primary purpose is to enable the sharing of user-generated material. Such a gaming service would also not be "a gaming service with limited communications functionality" since the definition for that type of service only includes services that enable gameplay "without enabling" the sharing of user-generated material.

An example of where this could arise is when a game allows users to share user-generated images, although it would not be the primary functionality of the game, e.g. an avatar. It would not be uncommon for video games to feature an avatar, which may be user-generated, in a leader board. In this scenario, the primary purpose is not for sharing user-generated material but an incidental feature.

A considerable proportion of gaming services may not fall under either category of gaming services in the Draft RES Standard. We suggest that it was not the policy intention for this scenario to occur that would create regulatory uncertainty, place onerous obligations, and lead to sub-optimal outcomes for providers of gaming services (that may not clearly fall under either gaming service category) to undertake a risk assessment.

We believe that adding the phrase "primary functionality" was a deliberate drafting decision by eSafety and intended to further delineate the definition of gaming services with

communications functionality.[5] To that end, we propose to amend the definition of gaming services with limited communications functionality to eliminate the potential gap between the two definitions. If that were not the intention of eSafety, we would appreciate the opportunity to have a conversation to understand the intent underlying the revised definitions and discuss solutions to clarify the definitions accordingly.

Recommendations:

- **To provide greater clarity while still addressing the policy intention, we propose an amendment to the definition of "a gaming service with limited communications functionality" (as was clearer in the Draft RES Code submitted for registration) to better enable a service provider to distinguish whether it falls under either a gaming service with communications functionality or limited communications functionality, and to ensure that there are no gaps between the two definitions of gaming services, i.e. to ensure clarity that a gaming service falls within one definition or the other. This could be amended along the following lines**:

  gaming service with limited communications functionality means a relevant electronic service, other than a closed communication relevant electronic service, the primary functionality of which is to enable end-users in Australia to play online games with other end-users without **the primary functionality of the service being to enable** the sharing of user-generated URLs, hyper-linked text, images or videos between end-users (other than material of a kind referred to in paragraph (e) of the definition of gaming service with communications functionality in this subsection).

- **We would welcome the opportunity to discuss further with eSafety to understand the intent underlying the revised definitions for gaming services with communications functionality and those with limited functionality. This will enable the opportunity to co-develop workable solutions that clarify the definitions accordingly, as recommended above.**

2.2 Obligations for gaming services with communications functionality

If a gaming service is categorised as one with communications functionality, the obligations are quite onerous and akin to Tier 1 RES. In contrast, "a gaming service with limited communications functionality" is akin to Tier 3 RES.

In general, it is concerning that the many requirements for "a gaming service with communications functionality" are onerous and prescriptive, without regard to the service's specific risk level.

We appreciate the intention to provide regulatory clarity and certainty for service providers on whether they should be categorised as gaming services with communications

[5] In a subsequent discussion with eSafety, we understand that it differed from the policy intention to create potential gaps in the definition between gaming services with communications functionality and those with limited communications functionality. In fact, it was intended to provide more clarity, certainty and enforceability.

functionality and those with limited communications functionality. However, some flexibility should be allowed in the circumstance where gaming services meet the definition of those with communications functionality, aligned with a more proportionate risk-based approach that promotes and incentivises a Safety-by-Design approach for "a gaming service with communications functionality".

There are already well-established principles for conducting risk assessments based on severity and probability of harm. Communications functionality can significantly vary from one gaming service to another. The severity and likelihood related to child sexual abuse material (CSAM) or pro-terror material (PTM) can be influenced by many factors including: whether the communication is transient; who plays the particular game or uses the particular service; effectiveness of existing measures already in place; and the types of communications possible.

As a potential solution, if a service provider were deemed to be "a gaming service with communications functionality" (and therefore subject to associated obligations), they should be given a rebuttable assumption. That is, they should be given the option to undertake a risk assessment to prove that they have a different risk profile, such as Tier 2 or 3 (and subject to those associated obligations). Alternatively, the service provider may elect not to undertake a risk assessment and accept the default obligations of "a gaming service with communications functionality".

Such an approach would balance between providing regulatory certainty and clarity in the operation of the RES Standard insofar as they apply to the categories for gaming services while offering some flexibility for gaming service providers who are categorised as having communications functionality to prove – if they choose to do so – that their risk level is proportionately targeted.

Recommendation: Where a gaming service meets the definition of a gaming service with communications functionality, the service provider should be given the choice to undertake a risk assessment as a rebuttable assumption to prove that they have a lower level of risk (and therefore subject to obligations according to their actual level of risk). Otherwise, they would be subject to the default obligations for gaming services with communications functionality.

3. Risk assessments

Discussion Paper Question 1: Are the requirements for risk assessment in the draft Standards targeted at the right services and at the right points in a service's development journey? Are the risk factors appropriate?

Concerning question 1, Part 3 of the Draft RES Standard includes requirements for risk assessments and determining risk profiles of RES, which would apply to RES that are not exempt. In the case of video games, a gaming service with communications functionality or limited communications functionality would be exempt (sections 8(6)(a) and (b)).

However, to respond to Question 1, there are fundamental questions regarding whether the gaming service definitions capture all gaming services and whether automatically presuming "a gaming service with communications functionality" should be treated as equivalent to Tier 1 RES, as discussed in section 2 above.

Further, there may be a scenario in which a service does not have an initial risk assessment requirement but may have to undertake one should there be material changes to that service (section 8(5)). This appears to be a drafting error.

Recommendations:

- **The appropriateness and relevance of the risk assessment requirements is contingent on further clarification of the definitions for gaming services with communications functionality, and gaming services with limited communications functionality.**
- **Section 8(5) should be amended so that a RES, which is not required to undertake an initial risk assessment, should be exempted from risk assessment requirements (similar to the services listed under section 8(6)) if there are material changes to the service.**

4. Policy considerations

Discussion Paper Question 2: Do the obligations on each relevant electronic service and designated internet service category appropriately reflect the above considerations? Are other considerations relevant?

With respect to question 2, the Discussion Paper lists the following considerations that eSafety has taken into account in setting out the proposed obligations:

- *the importance of striking a balance between flexibility and enforceability, so service providers, eSafety and third parties have clarity about required outcomes*
- *the principle of risk-based, outcomes-based and technology neutral regulation so providers can implement measures that reflect the characteristics of their service and are responsive to rapidly shifting technologies*
- *ensuring obligations are meaningful as well as technically feasible, practical and – where appropriate – able to be deployed at scale*
- *the importance of human rights, including the right to freedom of expression, the right not to be subjected to arbitrary or unlawful interference with privacy, the right to protection from exploitation, violence and abuse, and the rights and best interests of children.*

We support the above considerations identified in the Discussion Paper. However, we consider that there are several obligations in the Draft RES Standard that need to take these considerations into account sufficiently. These themes are discussed further throughout this submission.

Among other concerns, several requirements fail to strike the appropriate balance between flexibility and enforceability, are not appropriately risk-neutral, and must be more practical as applied to online gaming services.

Recommendation: Addressing the matters raised in our submission should contribute to better reflecting eSafety's policy considerations in setting out proposed obligations in the RES Standard. In its current form, the requirements do not strike the appropriate balance between flexibility and enforceability, not risk neutral, and not practical with respect to online gaming services.

5. Applicability

Discussion Paper Question 3: Is the test in section 5 workable? Is further guidance required to assist providers to determine whether this standard, or another code or standard, applies to a particular online service?

5.1 Applicability of the RES Standard

In response to question 3, we are of the view that the RES Standard is the governing document for online video game services, in accordance with section 5 of the Standard. That is, gaming services have been explicitly defined in the Standard and the predominant functionality of the service is more closely aligned with the Draft RES Standard than with the Draft DIS Standard. We understand that the only compliance requirements applicable to online video gaming services are those contained in the RES Standard and that none of the compliance requirements in any of the Codes or the DIS Standard apply to online video game services. Hence, we have only commented on the Draft RES Standard. Should eSafety determine otherwise, we would welcome further guidance from eSafety.

Recommendation: We are of the view that the RES Standard is the standard applicable to online video games and that no other code or standard applies. Should eSafety determine otherwise, we would welcome guidance.

5.2 Alignment with the National Classifications Scheme

As a general comment regarding the applicability of relevant legislation and regulations, we note that there have been several instances in which the Draft RES Standard provides specific definitions related to Class 1A and 1B material, e.g. CSAM, child sexual exploitation material, extreme crime and violence material, and PTM. This may be text that has been partially adopted or copied from the Head Terms of the Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material).[6]

[6] Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) – Head Terms (12 September 2023).

However, in moving from Codes to Standards, the Draft RES Standard omits some other key relevant information from Annexure A of the Code's Head Terms (Guidance on Classification Process). It is unclear whether eSafety will adopt the full content from this Annexure in subsequent guidance material.

As stated in Annexure A, it provides an overview of the Classification Process as it applies at the date of the Codes (12 September 2023). To the extent that the Classification Process changes, including as a result of any legislative reforms or changes to applicable supporting codes or guidelines, industry participants must refer to the updated Classification Process. The industry representatives responsible for leading the development of the Code must work to promptly update this Annexure as required to reflect any changes to the Classification Process. This Annexure includes direct extracts from relevant legislation and instruments, in addition to summaries and guidance prepared to assist industry.

At this stage, the Standard's omission of the full content of Annexure A, therefore, presents a risk of inconsistencies and misalignment with the National Classifications Scheme. This will become a more prominent issue if amendments are made to the Scheme, which the Draft RES Standard currently does not explicitly contemplate.

Recommendation: As a matter of good regulatory practice, 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 Class 1B Material), should be adopted in the Draft RES Standard to ensure regulatory coherence with the National Classifications Scheme and consistent with the Codes already registered by eSafety.

6. Technical feasibility and practical limitations

Discussion Paper Question 4: Is the technical feasibility exception in the obligation to detect and remove known child sexual abuse material and pro-terror material appropriate? How effective will this obligation be with this exception?

Discussion Paper Question 6: Are there any limitations which would prevent certain service providers from deploying systems, processes and technologies to disrupt and deter child sexual abuse material and pro-terror material on relevant electronic services? If there are limitations, how might these be overcome? Is it appropriate for this requirement to apply to gaming services with communication functionality?

Section 7 of the Draft RES Standard covers technical feasibility. In response to questions 4 and 6, several issues arise from the operation of this provision (in addition to others) that may not be appropriate in practice.

6.1 Encryption

We understand that it is not eSafety's policy intention for end-to-end encryption to be broken through implementing its online safety standards.[7] While we welcome such assurances, it can be argued that the current drafting of section 7 in the Draft RES Standard could inadvertently break encryption without any explicit provision.

Section 7 in the Draft RES Standard currently reads as follows:

> **7 Technical feasibility**
>
> In considering whether it is or is not technically feasible for the provider of a relevant electronic service to take a particular action, the matters to be taken into account include:
> (a) the expected financial cost to the provider of taking the action; and
> (b) whether it is reasonable to expect the provider to incur that cost, having regard to the level of the risk to the online safety of end-users in Australia of not taking the action.

This issue extends to other provisions in the Draft RES Standard, such as sections 20(3) and (6) relating to measures to detect and remove known CSAM, where encryption may be broken because the definition of "technically feasible" could be open to interpretation. Clarification in the Standard and guidance will be necessary to clarify how these might apply to avoid breaking encryption. Otherwise, this could present a risk to service providers and their customers.

In contrast, section 6.1 of the Code's Head Terms explicitly took into account protecting security (as well as other essential safeguards such as privacy and confidentiality). It is unclear whether eSafety will adopt this in subsequent guidance material.

Recommendations:

- **Section 7 of the Draft RES Standard should be amended to reflect eSafety's intention that encryption will be protected, along with further guidance.**
- **Section 6.1 of the Code's Head Terms should be applied to reflect a broader set of principles that preserve security of online services.**

6.2 Pro-terror material

It can be argued that the detection and removal of pro-terror material (PTM) is not as obvious as CSAM.[8] PTM requires more context and is subject to the determination of the relevant jurisdiction as to whether the material should be classified as pro-terror. Additionally, unlike CSAM, the harm associated with PTM stems from consumption rather than generation and simply holding the material. Further thought is required to consider how PTM is defined and managed in practice. Requirements to proactively detect and

[7] Statement on end-to-end encryption and draft industry standards | eSafety Commissioner.

[8] In a subsequent discussion with eSafety, we understand that PTM was not intended to apply to gaming services under the Draft RES Standard, although it has been included in the Draft RES Standard.

report PTM should only apply where this material is shared with other users and represents a real-world threat.

The previous Draft RES Code acknowledged that there may be statutory obligations in this domain, but it has been omitted in the Draft RES Standard.[9] Nevertheless, it would seem inappropriate for a service provider to be made responsible in assessing PTM as a proxy for the role of law enforcement.

Recommendation: Rather than placing the responsibility solely on the service provider, eSafety should give further direction as to how PTM is determined, the relevant jurisdiction that decides on whether it is PTM, and the role of law enforcement agencies in assessing PTM. This is particularly given the nuance required to appropriately assess such material, which has been strongly exemplified with the current conflict in the Middle East. For example, the definition proposed in the rejected Draft RES Code had the condition that PTM means material that is Refused Classification (RC) or would be RC if assessed for classification by the Australian Classification Board.

6.3 Disrupting and deterring CSAM and PTM

Section 22 of the Draft RES Standard covers disrupting and deterring CSAM and PTM and applies to a pre-assessed RES (such as "a gaming service with communications functionality") and a Tier 1 RES. Under this provision, service providers must implement systems, processes and technologies that effectively deter and disrupt users from using the service to create, offer, solicit, access, distribute, or otherwise make available or store CSAM or PTM (section 22(2)). Systems, processes, and technologies may include hashing, machine learning, AI and other tools that scan for known CSAM or PTM, and tools designed to detect key words, behavioural signals and patterns associated with CSAM and PTM (section 22(3)).

The provision raises several questions that require attention, including:

- Effectively deter and disrupt: This requirement is both unclear and potentially impossible to comply with. For instance, what would satisfy the requirements for "effectively deter and disrupt"? Is a filtering tool required and sufficient? Does it have to be foolproof, which is not realistically achievable? We note that this was not a requirement in the Codes, so there is no context and background to understand the

[9] We note that the previous Draft RES Code acknowledged the role of RES to facilitate private communication between end-users, with the measures in the Code designed to be respectful of Australian end-users' legitimate expectations around the privacy and security of those communications and to ensure that measures do not contravene statutory obligations that are applicable to the providers of relevant electronic services. These statutory obligations may include: the *Privacy Act 1988* (Cth); Part 13 of the *Telecommunications Act 1997* (Cth); the *Telecommunications (Interception and Access) Act 1979* (Cth); various laws relating to unauthorised access to data/computers; and various laws relating to surveillance. These do not appear to be included in the Draft RES Standard.

rationale behind this requirement. The requirements should be clarified that they are underpinned by conduct that demonstrates acting in good faith and best endeavours to implement achievable solutions, avoiding language that is both vague and built on absolutes.

- Offering and soliciting: The obligation for service providers to deter and disrupt users against "offering" and "soliciting" CSAM and PTM will be difficult to implement in practice, especially subject to what would be deemed as sufficient by eSafety. This obligation could be interpreted as requiring service providers to actively scan for text and voice communications that could be considered solicitations or offers to distribute CSAM or PTM outside the service providers' platforms.
- Behavioural signals and patterns: The meaning of "behavioural signals and patterns" associated with CSAM and PTM is undefined and unclear. Without clarity, this may be difficult to detect in online game environments and may unintentionally cause under-moderation or, alternatively, overreach.
- Proportionality: How would these requirements differ between services that have higher or lower probabilities of actually being used to create, offer, solicit, access, distribute, or otherwise make available or store CSAM or PTM?

Recommendations:

- **Section 22 requirements for disrupting and deterring CSAM and PTM need further clarification, especially in the context of video games.**
- **With respect to the reference to "behavioural signals and patterns associated with CSAM and PTM", consideration should be given to either deleting or significantly redrafting this requirement, as it is currently vague in meaning and relevance.**

7. Examples of industry practices

Discussion Paper Question 5: Are there other examples of systems, processes and technologies that can detect, flag and/or remove known child sexual abuse material and known pro-terror material at scale, which should be highlighted in the Standards or accompanying guidance?

Discussion Paper Question 7: Are there other examples of systems, processes and technologies that can disrupt and deter the use of a relevant electronic service to solicit, generate, distribute or access child sexual abuse material and pro-terror material, which should be highlighted in the guidance?

In response to questions 5 and 7, the video game industry (as a whole and globally) takes consumer protection extremely seriously, offering high levels of safeguards so players and parents can enjoy video games fun and responsibly. The industry adheres to strict domestic and international data and consumer protection laws, supplemented with an age-appropriate video game content labelling scheme, along with other measures. The industry

also leads in empowering players and parents with easy-to-use tools, including for managing playtime, spending, online privacy, and access to age-appropriate games.

The industry's serious commitment and responsibility to these protections are built around global industry best practices, according to the following pillars: age-appropriate pre-contractual information; safety by design in online environments; tools to enable players, parents, and caregivers to set the permissions that are appropriate for them or their children; and enabling consumer redress and efficient and proportionate enforcement.

Recommendation: The video games industry takes online safety extremely seriously and follows global industry best practices in implementing community protections. IGEA would welcome the opportunity to share with eSafety activities that support eSafety's objectives.

8. Development programs

Discussion Paper Question 8: Do you agree with the monthly active user threshold for the investment obligation? Are there other appropriate thresholds that should be considered to ensure the obligation is proportionate to the size and reach of the relevant electronic service?

Concerning question 8, section 23 of the Draft RES Standard covers development programs and applies to a pre-assessed RES (such as "a gaming service with communications functionality") and a Tier 1 RES, where the average monthly number of active end-users of the service in Australia over the previous financial year was one million or more (section 23(1)). Service providers must have a program of investment in and development activities designed to detect and identify, and deter the distribution of CSAM and PTM on the service, and for cooperating and collaborating with other organisations involved in CSAM and PTM detection and deterrence (sections 23(2) and (3)). There is also a requirement for investment and activities to reduce the risk in relation to "synthetic material generated by AI". The provision also includes examples of activities and investments that may be part of a service provider's development program.

Several issues with this investment obligation require attention:

- Rationale: The threshold proposed for determining whether a service provider should be subject to an investment obligation for development programs requires further thought. For instance, in its current form, the investment obligation does not incentivise service providers to design inherently lower-risk services whenever possible (which could include using eSafety's Safety-by-Design principles). As noted earlier, treating "a gaming service with communications functionality" as equivalent to a Tier 1 service automatically assumes that such a gaming service is a high risk without evidence. Using arbitrary definitions and thresholds to regulate lower-risk and higher-risk services identically and with the same onerous requirements removes one of the potential incentives.

- Synthetic material generated by AI: The phrase "synthetic material generated by AI" is undefined, and therefore, the inclusion of the requirement for investment and activities to reduce the risk in relation to "synthetic material generated by AI" is unclear. Indeed, it is not clear what risk is contemplated by this requirement. On its face, this requirement is well outside the scope of the core purpose of the RES Standard, which targets Class 1A and 1B material. Thus, this component of section 23 should be deleted.

Recommendations:

- **eSafety should give further thought on the rationale of when a service provider should be subject to an investment obligation for development programs – a proportionate approach would be based on the level of risk of the service, as opposed to arbitrary definitions and thresholds.**
- **The reference to "synthetic material generated by AI" should be deleted under section 23, as it is undefined and unclear.**

9. Reporting obligations

Discussion Paper Question 9: Are the end-user reporting requirements workable for the relevant service providers? Are there practical barriers to implementation?

Discussion Paper Question 10: Should the requirement on certain relevant electronic services to respond to reports of class 1A and class 1B material on their service be limited to a requirement to take 'appropriate action'?

Questions 9 and 10 in the Discussion Paper focuses on end-user reporting obligations in the Draft RES Standard. Here, we also raise other issues relevant to the wider range of public reporting, notifications, and response obligations in the Standard.

9.1 Appropriate action

Sections 17 and 25 of the Draft RES Standard require certain RES (including "a gaming service with communications functionality") to take "appropriate action" to engage with reports of Class 1A and 1B materials and determine whether terms of use or policies have potentially been breached.

The term "appropriate action" is open to interpretation and can be too onerous without proper clarification. While section 12 discusses appropriate action, it ultimately refers to the Object of the Standard under section 4, which can be interpreted as having a broad meaning.

The Draft RES Code provided more clarity on what would be considered appropriate action for service providers. In particular, Measure 12 in the Code included examples of appropriate steps in response to breaches of policies, along with guidance.

Recommendation: To provide more clarity, the Draft RES Standard should reinstate what would constitute "appropriate action" from the Draft RES Code.

9.2 Notifying new features or functions

Section 35 of the Draft RES Standard applies to certain RES (including "gaming service with communications functionality") and covers the notification to eSafety by applicable service providers of new features or functions to their services. In particular, section 35 states:

> (2) If the provider of a service decides to add a new feature or function to the service, the provider must notify the Commissioner of the proposed change as soon as practicable after making the decision unless the provider considers, on reasonable grounds, that the proposed change will not significantly increase the risk that the service will be used to solicit, access, distribute or store class 1A material or class 1B material.
>
> (3) If a new feature or function is added to a service, the provider of the service must notify the Commissioner of the change as soon as practicable unless the provider determines, on reasonable grounds, that the change has not significantly increased the risk that the service will be used to solicit, access, distribute or store class 1A material or class 1B material.

There are several practical issues with this notification requirement that require attention:

- Lack of context: This is a new requirement introduced into the RES Standard. In the absence of an explanation behind the rationale for the inclusion of this new requirement, it is difficult to understand the necessity for this provision.
- Regulatorily burdensome approach: If this notification requirement is widely interpreted, it would apply to any new feature or function reacted to the service, which would be significantly burdensome to implement in practice. For instance, this could require the service provider to: introduce a process for reviewing all new features for risk (including immaterial or minor changes); implement procedures across every game and service to make sure those features pass through a process once a new feature has been decided upon (and then also after being added); and documentation of the service provider's decision and rationale for determining a new feature does not increase risk, and whether or not the Commissioner will need to be notified. The burden of this requirement is entirely disproportionate to the risk of harm and the potential benefit. It significantly interferes with the ordinary course of business and service development. It also poses a significant potential competitive risk if a business must notify eSafety of every new feature it has decided to implement.
- Unnecessary dual notification: Requiring a service provider to notify the Commissioner after the service provider decides to add a new feature *and* then after actually adding a new feature is duplicating efforts and is an unnecessary intrusion into the business operations of service providers.

The Draft RES Standard already includes sufficient safeguards regarding new features or functions under section 19 that would not necessitate section 35. Section 19 requires the

service provider to implement safety features and settings before the service provider makes a material change to its service. This entails the provider assessing and incorporating features to minimise the risk of Class 1A and 1B material.

Recommendation: The requirement for notifying new features or functions under section 35 should be considered redundant and removed, as it is already covered by section 19 in the Draft RES Standard.

9.3 Reporting obligations to eSafety

We note that there are several reporting requirements for service providers to eSafety. These include reporting obligations on outcomes of the development programs (section 36) and annual compliance reports (section 37).

As a matter of good regulatory practice, safeguards should be in place to ensure due process, transparency, confidentiality, and privacy concerning reporting obligations. Currently, the Draft RES Standard does not explicitly offer these protections. For example, disclosure of a service provider's number of active users (section 37(3)(a)) in Australia could be regarded as commercially sensitive and anti-competitive, while offering no value to reporting about online safety.

Further, the purpose of the reporting requirements needs to be clarified. For instance, to ensure that service providers comply with their obligations, section 38 enables the Commissioner to require compliance reports (amongst other things) from the service provider. This renders the annual compliance reporting requirement under section 37 redundant and superfluous.

If the intention is to promote transparency, trust, and collaboration, it is important to treat any information shared with eSafety in good faith. This, therefore, requires appropriate safeguards to be put in place to enable due process, e.g. the right to be heard and transparency in how a service provider's information will be published and reported by eSafety.

If the Commissioner intends to use the reports as a naming-shaming tool, there should be appropriate steps in place to ensure that service providers are provided with an opportunity to redress any compliance issues before resorting to regulatory action.

Recommendations:

- **The requirement for proactive annual compliance reports from service providers under section 37 should be removed, as section 38 empowers the Commissioner to require compliance reports more generally. Where specific requirements under section 37 is practicable and achievable, in consultation with relevant service providers, these could be incorporated into section 38 reporting requirements.**

- **The reporting obligations in the Draft RES Standard should be built upon appropriate safeguards that promote due process, transparency, confidentiality and privacy.**

10. Compliance costs

Question 11: What are your views on the likely compliance costs and, in particular, the impact of compliance costs on potential new entrants?

Generally, while any form of new regulation is costly for larger providers, for smaller companies (let alone new entrants) any new regulation will likely have a greater disproportionate impact. Government uplift in regulatory cost support might be beneficial (e.g. tax exemptions for purchasing new technologies or investing in capabilities and measures that assist in addressing these obligations).

In response to question 11, for a proper compliance costs assessment, additional clarification will be required regarding the operation of certain proposed new provisions in the Draft RES Standard, such as through guidance material omitted from consultation at this stage. These do not account for the regulatory costs of other reforms that may cover similar issues but from different regulatory angles, e.g. privacy requirements, etc.

Recommendations:

- **For a proper compliance costs assessment, additional clarification will be required regarding the operation of certain proposed new provisions in the Draft RES Standard such as through guidance material that has been omitted from consultation at this stage.**
- **We strongly recommend that eSafety undertakes further consultation on the associated draft guidance material for the Draft Standard.**

Thank you for providing IGEA with an opportunity to contribute to eSafety's consultation on the Draft RES Standard. For more information on any issues raised in this submission, please contact IGEA's Director of Public Policy & Government Relations, Charles Hoang, at [redacted] or policy@igea.net.