9 February 2023

Louise Hyland
Chief Executive Officer
Australian Mobile Telecommunications Association

Victoria A. Espinel
President and CEO
BSA | The Software Alliance

John Stanton
Chief Executive Officer
Communications Alliance

Sunita Bose
Managing Director
Digital Industry Group Inc

Ron Curry
Chief Executive Officer
Interactive Games & Entertainment Association

By email: at [redacted] **and** [redacted]

Invitation to respond and/or submit amended draft code – Relevant Electronic Services

Dear Louise, Victoria, John, Sunita and Ron,

On 18 November 2022, I received a request from the six industry associations making up the Steering Group (**Steering Group**) to register the Consolidated Industry Codes of Practice for the Online Safety Industry (Class 1A and Class 1B Material) purusant to section 140 of the *Online Safety Act 2021* (Cth) (**the Act**).

As presented, the Consolidated Industry Codes comprise a set of head terms, and eight separate industry codes that apply to different sections of the online industry. In the request for registration, the Australian Mobile Telecommunications Association, BSA | The Software Alliance, Communications Alliance, Digital Industry Group Inc and the Interactive Games and Entertainment Association (collectively, the **Industry Bodies**) indicated that together they represent providers of relevant electronic services and were responsible for developing the Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material) (**draft RES Code**).

Section 140 of the Act gives me, as the eSafety Commissioner, power to register an industry code. I have considered the relevant requirements under the Act, taking into account the Steering Group's submission and accompanying documents.

I have not yet made a decision whether to register the draft RES Code, but have formed a preliminary view. The **attached** statement sets out my preliminary views on the draft RES Code and provides you with an opportunity to respond and/or submit an amended draft code before I finalise my decision. Separate letters are being sent to the relevant industry associations relation to each draft industry code.

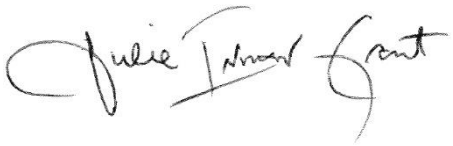
If I decide not to register a code for a section of the online industry, I intend to determine an industry standard under section 145 of the Act for that section of the online industry.

Next steps

I invite you to respond to this letter and/or submit an amended draft RES Code by 5pm AEDT on 9 March 2023.

If you have any questions about this letter, please contact Morag Bond, Executive Manager, Legal MarComms and Research on [redacted], Vicki Buchbach, Co-Manager, Industry Codes team, on [redacted], or the eSafety Industry Codes Team at [redacted]

Yours faithfully,



Julie Inman Grant
eSafety Commissioner

Statement of Preliminary Views – Relevant Electronic Services (RES) Code

Summary

On the information currently available, the eSafety Commissioner's preliminary view is that:

- the draft RES Code does not meet the requirement under s 140(1)(b) of the Act, because the code is expressed to apply in respect of "Australian end-users" rather than "end-users in Australia",
- the draft RES Code also does not meet the requirement under s 140(1)(d) of the Act, because it does not provide appropriate community safeguards for matters of substantial relevance to the community (as identified in the Request for registration), namely Matters 1, 2, 6, and 11, and
- as a consequence of these issues, the eSafety Commissioner's jurisdiction to register an industry code under s 140(2) is not enlivened.

The Industry Bodies are invited to provide a response to this Statement of Preliminary Views and submit an amended industry code addressing the areas of concern set out below.

Background

1. On 11 April 2022, the eSafety Commissioner (**eSafety**) issued a notice to the Industry Bodies, requesting the development of an industry code that applies to participants in the group consisting of providers of relevant electronic services, so far as those services are provided to end-users in Australia (as defined under s 135(2)(b)).
2. The notice required an industry code dealing with specified matters to be submitted to eSafety by close of business on 9 September 2022. By variation issued on 24 June 2022, eSafety extended the due date for submission of the industry code to 18 November 2022.
3. By email dated 18 November 2022, Industry Bodies submitted the draft RES Code to eSafety for registration. Accompanying the draft RES Code were a cover letter, an explanatory document titled 'Request for registration', and a submission log from the public consultation and industry associations' responses to public consultation.

Section 140 requirements

4. eSafety has reviewed the Industry Bodies' submission including the accompanying documents. eSafety has also closely considered the draft RES Code in light of previous discussions between eSafety and members of the Steering Group, as well as other factors such as current industry practice, the systems and technologies available and used by RES providers as well as the policies and procedures currently adopted, international approaches, government and NGO reports. eSafety has closely considered the effectiveness and the enforceability of the proposed compliance measures.
5. Section 140(1) of the Act sets out the conditions which must be met in order to enliven eSafety's discretionary power under s 140(2) to register a code. Based on the information currently available, eSafety is unlikely to be satisfied that all of the conditions in s 140(1) are met. Consequently, the

power to register an industry code under s 140(2) of the Act would not be enlivened. The reasons for this are set out below.

Section 140(1)(b) requirement

6. Section 140(1)(b) of the Act requires eSafety to be satisfied that an industry code submitted by a body or association referred to in s 140(1)(a) applies to participants in that section of the online industry and deals with one or more matters relating to the online activities of those participants.
7. The relevant 'section of the online industry' is the group consisting of providers of relevant electronic services, so far as those services are provided to end-users in Australia, as described in s 135(2)(b).[1]
8. The relevant 'online activity' for the draft RES Code is providing a relevant electronic service, so far as the service is provided to end-users in Australia, as described in s 134(b).
9. Clause 2 of the draft RES Code stipulates its scope 'applies to relevant electronic services to the extent provided to Australian end-users'.
10. eSafety considers 'end-users in Australia' and 'Australian end-users' are materially different concepts, despite the likely overlap, because the former reflects the end-user's geographical location, while the latter (as defined in the head terms) reflects the ordinary residency status of the end-user.
11. While some parts of the Act refer to 'Australians' and 'end-user' who is 'ordinarily resident in Australia', the provisions identifying the online activities subject to the proposed codes (ss 134-135) are not expressed in these terms. eSafety considers that the registration criteria in s 140 must be considered by reference to ss 134-135.
12. eSafety considers it unlikely that the draft RES Code would satisfy s 140(1)(b) of the Act because the code is expressed to apply in respect of 'Australian end-users' and not to the relevant group of providers, described in s 135(2)(b), or to the relevant online activity, described in s 134(b).

Section 140(1)(d) requirement

13. Section 140(1)(d)(i) of the Act requires eSafety to be satisfied that, to the extent to which the draft RES Code deals with one or more matters of substantial relevance to the community, the code provides appropriate community safeguards for that matter or those matters.
14. eSafety considers that the draft RES Code, as submitted, is unlikely to meet the requirement under s 140(1)(d)(i) of the Act, because it does not provide appropriate community safeguards for Matters 1, 2, 6, and 11 for the reasons outlined below.

[1] For the avoidance of doubt, eSafety is satisfied at this stage that the requirement under s 140(1)(a) that the Industry Bodies represent providers of relevant electronic services, so far as those services are provided to end-users in Australia, has been met. This Statement of Preliminary Views relates only to the scope of the draft RES Code as submitted.

Matter 1

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to detect and prevent access or exposure to, distribution of, and online storage of class 1A material.

15. The draft RES Code proposes minimum compliance measures (**MCMs**) 1 – 11 and optional compliance measure (**OCM**) 12 to deal with Matter 1.

16. eSafety considers that the proposed MCMs are positive steps towards addressing the harm associated with some child sexual abuse materials (**CSAM**) and pro-terror materials. However, in order to provide appropriate community safeguards for Matter 1, the draft RES Code would need to ensure, at a minimum, that:

    (a) the commitment in MCM 5 for Tier 1 and Tier 2 RES to take appropriate action in response to breaches of policies for prohibiting Child Sexual Exploitation Material (**CSEM**) and pro-terror material should require appropriate action to be taken in relation to breaches of policies prohibiting other class 1A material;

    (b) Closed Communication RES and Encrypted RES should also be subject to MCM 5;

    (c) all Tier 1 RES (regardless of whether they meet the definition of Very Large RES), should commit to use appropriate systems, processes and technologies to detect and remove known CSAM (MCM 9)

    (d) Closed Communication RES and Encrypted RES should commit to use appropriate systems, processes and/or technologies to detect and remove known CSAM (MCM 9) (recognising that services using carrier networks are limited in their ability to deploy relevant technologies but other technologies, systems or processes could be implemented to detect and remove known CSAM and known pro-terror material);

    (e) all Tier 1 RES (regardless of whether they meet the definition of Very Large RES), Closed Communication RES and Encrypted RES should commit to use appropriate systems, processes and/or technologies to detect and remove known pro-terror material/Terrorist and Violent Extremist Content (**TVEC**) where available (MCM 10);

    (f) Tier 1 RES and Dating services should commit to ongoing investment in systems and process and technologies in relation to the detection of class 1A material (including first generation CSAM). The commitment should not be limited to a commitment to invest in the safe design of its services to 'provide appropriate support for the *provider's compliance with this Code*' in order to ensure there is ongoing investment to address the broader risk of class 1A content on services (including first generation CSAM); and

    (g) Closed Communication RES and Encrypted RES should commit to ongoing investment in systems, process and/or technologies in relation to the detection of class 1A material (including first generation CSAM). The commitment should not be limited to a commitment to invest in the safe design of its services to 'provide appropriate support for the *provider's compliance*

with this Code' in order to ensure there is ongoing investment to address the broader risk of class 1A content on services (including first generation CSAM).

17. While eSafety recognises that CSEM and pro-terror material are different to other types of class 1A material (in both the nature and extent of the harms and also the ability of this material to be more easily defined and/or identified), eSafety disagrees with the limited application of MCM 5, which requires action in response to breaches of policies prohibiting CSEM and pro-terror material, to a subset of class 1A material. Under the Act, eSafety is empowered to issue removal notices for the removal of all class 1 material with a requirement to comply within 24 hours. In order to provide appropriate community safeguards, the draft RES Code should complement this complaints and removal scheme; confining the commitment in MCM 5 to CSEM and pro-terror material risks undermining it.
18. In order to provide appropriate community safeguards, MCM 5 should also apply to Closed Communication RES and Encrypted RES. Without such a commitment, there is no requirement on Closed Communication RES and Encrypted RES to enforce, apply or adhere to their terms of use or policies prohibiting CSEM, pro-terror or the broader category of class 1A content. Commitments to have systems and processes *enabling* RES providers to respond to breaches are unlikely to be effective without a commitment to use them and apply their policies. To avoid any doubt, eSafety is not suggesting that such providers commit to taking certain steps (such as terminating an end-user's account) in relation to all class 1A material. As currently drafted, other than the removal of identified CSEM and pro-terror material, MCM 5 does not prescribe specific steps that the service provider must take. eSafety's view is that this drafting reduces the potential consequences of an overly rigid or inflexible approach.
19. Further, eSafety considers that all Tier 1 RES (regardless of whether they meet the definition of Very Large RES) could reasonably comply with a requirement to use appropriate systems, processes and technologies to detect and remove known CSAM (MCM 9).
20. Recognising that encrypted services and services using carrier networks may be limited in their ability to deploy relevant technologies, eSafety considers that Encrypted RES and Closed Communication RES could reasonably comply with a requirement to use systems, processes and/or technologies to detect and remove known CSAM (MCM 9) and that such a commitment is important to provide appropriate community safeguards.
21. eSafety considers that Tier 1 RES (regardless of whether they meet the definition of Very Large RES), Closed Communication RES and Encrypted RES should use appropriate systems, processes and/or technologies to detect and remove known TVEC/pro-terror material (MCM 10). While this commitment would not require providers to use all three of systems and processes and technologies, eSafety notes that in practice, some RES providers may use the same systems, processes and technologies to detect and remove known TVEC as they do for known CSAM (while using different datasets).
22. There are multiple ways these broadly drafted requirements (which do not require the deployment of specific technology) could be met, including options appropriate for less well-resourced businesses. For services able to use hash matching, there is a mix of proprietary and open-source hash matching

tools that are widely used (we note over 200 organisations use PhotoDNA). Hash matching is considered a privacy-preserving method with minimal risk of false positives.[2]

23. RES providers have the option to work with a recognised Non-Governmental Organisation to access hash databases. There are several databases of CSAM hashes with the largest database held by National Center for Missing and Exploited Children (**NCMEC**). While the only current database of known TVEC accessible by multiple companies is held by the Global Internet Forum to Counter Terrorism (**GIFCT**), eSafety also understands Meta and Google recently introduced tools to help combat the spread of terrorist content and will make these available to a wide range of companies for free.

24. Alternatively, RES providers could consider working with or joining Tech Against Terrorism, using the Terrorist Content Analytics Platform (as several do already) which is designed with the aim of supporting smaller tech platforms, including by sharing alerts for known TVEC URLs. Providers could also make use of proprietary technologies or develop their own tools aimed at detecting, for example, material associated with proscribed terrorist organisations based on Australian law or international reference points such as the UNSC Consolidated Sanctions List, including ensuring that content reported to their platform is not re-uploaded.

25. eSafety recognises that for some services (e.g. Encrypted RES) there are inherent limitations in the types of technologies that can be effectively deployed. However, the commitments in MCMs 9 and 10 are broad in terms of the options available to service providers to meet the requirement.

26. The commitment to make ongoing investments in the safe design of services that provide appropriate support for the provider's compliance with this Code (MCM 11) appears to effectively confine the scope of any investment required to the performance of the existing commitments. This means there is no commitment to invest in systems, processes and technologies to detect content such as first generation (new) CSAM. Given the immensely harmful consequences associated with the creation, distribution and dissemination of first generation CSAM as well as the development and increasing deployment of technologies and processes aimed at detecting first generation CSAM, the limitation of this investment commitment does not seem reasonable and appears unlikely to provide appropriate community safeguards.

27. Further, MCM 11 does not include Closed Communication RES, Encrypted RES and Dating services. eSafety considers it reasonable for these services to commit to making ongoing investments, particularly given the flexibility the guidance of MCM 11 provides to make ongoing investments that vary depending on the type of service. Without such commitments, eSafety is concerned that appropriate community safeguards may not be provided.

28. Technologies and processes which detect first generation CSAM and TVEC are increasingly being developed and deployed on services. eSafety considers that commitments by Tier 1 providers and Dating services to invest in the development and/or deployment of such technology is critical in order

[2] Testimony of Dr Hany Farid to House Committee on Energy and Commerce Fostering a Healthier Internet to Protect Consumers, 2019: www.congress.gov/116/meeting/house/110075/witnesses/HHRG-116-IF16-Wstate-FaridH-20191016.pdf

to provide appropriate community safeguards. eSafety also considers it important for the commitment to cover investment in systems and processes and technologies, given processes and systems (potentially incorporating human moderation) will need to sit alongside technologies. This approach increases the effectiveness and enforceability of this commitment.

29. eSafety notes that the commitments made in relation to Matter 1 fall short of the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (the **Principles**),[3] which reflect collective resolve and have been endorsed by multiple technology companies since 2020 including Apple, Google, Match Group, Meta and Microsoft (eSafety notes that the services provided by these companies include Tier 1, Very Large Tier 1, Dating services, Closed Communication RES and Encrypted RES). The Principles were developed in conjunction with industry representatives, and in consultation with a broad range of experts from civil society and academia as part of a global response designed to apply across different services. The Principles are supported by the Five Country governments (Australia, Canada, New Zealand, UK and US) and the G7. In particular, the Principles endorsed by the companies include identifying and combating the dissemination of **new** child sexual abuse material via their platforms and services, and to consider where existing measures can go further and to invest in innovative tools and solutions (e.g. Principle 2).

Matter 2

Measures directed towards achieving the objective of ensuring that industry participants have scalable and effective policies, procedures, systems and technologies in place to take reasonable and proactive steps to limit access or exposure to, and distribution of class 1B material.

30. The draft RES Code proposes MCMs 13 – 16 to deal with Matter 2.

31. eSafety is concerned with the scope and application of MCM 14. While this measure does not list class 1B material specifically it refers generally to 'breaches of terms and conditions, community standards, and/or acceptable use policies'.

32. eSafety recognises that these measures in the draft RES Code are designed to be proportionate to the relative harmfulness of class 1B material compared to class 1A. However, eSafety is concerned with MCM 14's limited application to Tier 1 and Tier 2 RES to take action in response to breaches of policies and the absence of such a commitment on Closed Communication RES and Encrypted RES.

33. In addition to this concern with MCM 14, eSafety is concerned with the omission of a specific reference to class 1B material and the range of examples of appropriate steps provided. eSafety is concerned that steps taken in accordance with this MCM will not work to complement eSafety's power under the Act to issue removal notices requiring removal of all material that is or would be classified as class 1.

34. These concerns are similar to those identified above by eSafety in relation to MCM 5.

[3] Principles, including signatories retrieved at: www.weprotect.org/library/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/

Matter 6

Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place which ensure communication and cooperation with the eSafety Commissioner with respect to matters about class 1A material and class 1B material, including complaints.

35. The draft RES Code proposes MCM 19 to deal with Matter 6.
36. The commitment in MCM 19 to share information with eSafety is limited to Tier 1 RES and Encrypted RES and it is not clear to eSafety why MCM 19 does not also include Closed Communication RES, given new features or functions could also change the risk profile for these services. eSafety's preliminary view is that, in order for MCM 19 to provide appropriate community safeguards, MCM 19 should be extended to Closed Communication RES.
37. eSafety's preliminary view is that the carve-out in MCM 19 excusing industry participants from providing confidential information in code reports is not appropriate and notes clause 7.3 (b) of the head terms. Clause 7.3(b) provides relevantly that 'if an industry participant identifies any material in a Code report as the industry participant's confidential information, eSafety must maintain such material in confidence'. Such information may clearly be of significance to eSafety's understanding of the risk of a service and eSafety would be expected to maintain the confidentiality of such information.
38. There is a minor issue with internal cross-referencing in MCM 19 as it cross-references MCM 28, which outlines annual reporting requirements for Tier 1 services. MCM 19 should also cross-refer to MCM 30, which outlines the reporting requirements for Closed Communications RES and Encrypted RES given the link between these two MCMs.

Matter 11

Measures directed towards achieving the objective of ensuring that industry participants publish annual reports about class 1A material and class 1B material, and their compliance with industry codes.

39. The draft RES Code proposes MCMs 28 – 31 to deal with this matter with Tier 1 RES providers subject to more specific mandatory reporting requirements (in MCM 28) than Tier 2, Closed Communication and Encrypted RES providers (MCMs 29-30). MCM 31 applies to Enterprise RES.
40. Under MCMs 29 and 30, Tier 2, Closed Communication and Encrypted RES providers are required to submit code compliance report to eSafety upon request. The report must be submitted within 6 months of receiving the request, although any request that would otherwise be due within the first 12 months after the code comes into effect is not due until 12 months after the code comes into effect. The head terms further provide that a code does not come into effect until 6 months after registration. This means that no reports would be due to eSafety until 18 months after registration at the earliest.
41. eSafety has concerns that the timeframe for responding to requests for reports under MCMs 29 and 30 will impact eSafety's ability to consider a service provider's compliance with code commitments, as well as eSafety's ability to provide constructive input into the first review of the RES Code, noting that all reporting data will be at least six months out of date. Further, without an effective review process, the capability of the RES Code to provide appropriate community safeguards may be compromised.

42. eSafety's preliminary view is that the proposed 6 months' response timeframe in MCMs 29 and 30 is likely to prevent these MCMs providing appropriate community safeguards in relation to this matter and suggests that a reasonable response timeframe of 2 months would be appropriate.

Enforceability of the code

43. In order to provide appropriate community safeguards under s 140(1)(d) of the Act, the head terms and the specific provisions in each industry code, when read as a whole, must be capable of being implemented and being enforced. This means ensuring service providers, eSafety and other parties have sufficient certainty and clarity about the obligations under the Codes. At the same time, eSafety recognises the importance of a balance between flexibility and ensuring compliance can be assessed and enforced.

44. eSafety has identified provisions in the head terms which are phrased and structured in ways that risk rendering the proposed compliance measures ineffective, or potentially impractical to measure and enforce. The following examples are not exhaustive:
Limitation clause in the head terms

- Clause 6.1 (c) limits the codes from requiring any industry participant to 'render methods of encryption or other information security measures less effective'. As previously communicated to Industry Bodies, eSafety has concerns that rendering 'other information security measures less effective' is too broad and is a very low bar. There is a risk that as drafted, clause 6.1(c) could create broad exclusions from code commitments. eSafety considers important that service providers consider how code compliance could be achieved by alternative mechanisms or by remedying the design.
- Clause 6.1 (e)(iii), (h), (i) and (j) and clause 6.2 each limit the codes from requiring industry participants to take action or engage in conduct that would violate other laws. As previously communicated to Industry Bodies, eSafety considers that the blanket exclusions are not desirable and it would be more appropriate for service providers to communicate specific concerns to eSafety when a specific issue arises as to how compliance with a code requirement may breach a law and/or explore alternative approaches to meeting the minimum compliance measures of the code while still meeting other legal requirements.

Risk assessment methodology

- In relation to the risk assessment methodology in the draft RES Code, eSafety is concerned that RES providers may underestimate their risk level if application of the tiers and relative weighting of the factors listed in the table is left to industry participants to determine without further guidance.
- The process to identify applicable compliance measures is entirely reliant on an effective risk assessment. While Tier 1, Tier 2, Closed Communication and Encrypted RES providers are required to demonstrate that the compliance measures they have adopted are reasonable, it would be difficult for eSafety to critically assess the risk profile assigned by the RES provider to

its online activity(ies) if those risk factors are open to broad interpretation and the risk profile adopted does not accurately reflect the risk of harm.

Notification of risk

- Under clause 5.2 of the head terms, eSafety may request advice of risk profiles. Tier 1 services are also required to notify eSafety that the service is in this Tier before the RES Code commences. eSafety considers that in the interests of clarity, there should also be a specific obligation on Very large RES providers to advise eSafety that their services fall within this subset of Tier 1.

Next steps

45. Industry Bodies are invited to respond to the Statement of Preliminary Views and submit an amended code that addresses all of the following:

    (a) the scope and application of the draft RES Code should align with the language of the Act where the relevant section of the online industry and relevant online activity are described by reference to 'end-users in Australia';

    (b) the commitment on Tier 1 and Tier 2 RES to take appropriate action in response to breaches of policies for prohibiting CSEM and pro-terror material (MCM 5) should be expanded to include taking appropriate action in relation to breaches of policies prohibiting other class 1A material. This commitment should also extend to Closed Communication RES and Encrypted RES;

    (c) commitments to implement systems, processes and technologies to detect, flag and remove known CSAM (MCM 9) should be mandatory for all Tier 1 RES (not just Very Large RES);

    (d) commitments to implement systems, processes and/or technologies to detect, flag and remove known CSAM (MCM 9) should be mandatory for Closed Communication RES and Encrypted RES;

    (e) commitments to implement systems, processes and/or technologies to detect, flag and remove known pro-terror material (MCM 10) should be mandatory for all Tier 1 RES (not just Very Large RES) and Closed Communication RES and Encrypted RES;

    (f) Tier 1 RES and Dating services should commit to ongoing investment in systems and processes and technologies in relation to the detection of class 1A material (including first generation CSAM). The commitment should not be limited to a commitment to invest in the safe design of its services to 'provide appropriate support for the *provider's compliance with this Code*' in order to ensure there is ongoing investment to address the broader risk of class 1A content on services;

    (g) Closed Communication RES and Encrypted RES should commit to ongoing investment in systems, processes and/or technologies in relation to the detection of class 1A material

(including first generation CSAM). The commitment should not be limited to a commitment to invest in the safe design of its services to 'provide appropriate support for the *provider's compliance with this Code*' in order to ensure there is ongoing investment to address the broader risk of class 1A content on services;

(h) the scope of the commitment in MCM 14 for Tier 1 and Tier 2 RES to take appropriate action in response to breaches of terms and conditions, community standards and acceptable user policies should be clarified to specifically refer to class 1B material. The commitment should also extend to include Closed Communication RES and Encrypted RES;

(i) the commitment to provide updates and consult with eSafety about new features (MCM 19) should refer to the correct measure for Encrypted RES (presumably MCM 30) and also be extended to Closed Communication services. The limitation excusing the provider from sharing information where it is confidential should be removed (noting there is no equivalent limitation in relation to Code reports);

(j) where the draft RES Code requires a code compliance report to be submitted within 6 months of receiving eSafety's request, the response timeframe should be revised to 2 months; and

(k) the Risk Assessment should be amended to include a specific obligation on providers of Very Large RES to advise eSafety if a service falls within this subset of Tier 1.

46. If Industry Bodies decide not to submit an amended code but wish to provide further information, the information should clearly explain how the MCM will, despite the express concerns identified above, provide appropriate community safeguards.

47. Any submission and revised code will need to be provided to eSafety by 5pm AEDT on 9 March 2023, in order for the eSafety Commissioner to take it into account before making her final decision. For the avoidance of doubt, eSafety makes no representations that an amended code addressing the above concerns will be registered by default.