

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

Ian McAlister
Chief Executive Officer
Consumers Electronics Suppliers' Association

Sunita Bose
Managing Director
Digital Industry Group Inc

Ron Curry
Chief Executive Officer
Interactive Games & Entertainment Association

By email: [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED] and [REDACTED]

Invitation to respond and/or submit amended draft code – Designated Internet Services

Dear Louise, Victoria, John, Ian, 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) pursuant 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, Australian Mobile Telecommunications Association, BSA | The Software Alliance, Communications Alliance, the Consumer Electronics Suppliers' Association, Digital Industry Group Inc and the Interactive Games & Entertainment Association (collectively, the **Industry Bodies**) indicated that together they represent providers of designated internet services and were responsible for developing the Designated Services Online Safety Code (Class 1A and Class 1B Material) (**draft DIS 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 DIS Code, but have formed a preliminary view. The **attached** statement sets out my preliminary views on the draft DIS Code and provides you with an opportunity to respond and/or submit an amended draft code before I finalise my decision. Separate letters will be sent to the relevant industry associations in relation to each draft industry code.

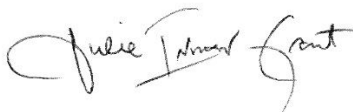
If I decide not to register a code for a section of the online industry, I intend to determine an industry standard under section 145 of the Act for that section of the online industry.

Next steps

I invite you to respond to this letter and/or submit an amended draft DIS 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], or Maggie Law, 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 – Designated Internet Services (DIS) Code

Summary

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

- the draft DIS 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 DIS Code 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, 4, 5 and 11, and
- as a result, the eSafety Commissioner’s jurisdiction to register an industry code under s 140(2) is not enlivened.

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 designated internet services, so far as those services are provided to end-users in Australia (as defined under s 135(2)(c)).
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 DIS Code to 18 November 2022.
3. By email dated 18 November 2022, the Industry Bodies submitted the draft DIS Code to eSafety for registration. Accompanying the draft DIS 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 DIS Code in light of previous discussions with members of the Steering Group, as well as other factors such as the current industry practice, the technological tools available and used by DIS providers (including end-user managed hosting services). eSafety has closely considered the effectiveness and 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, the eSafety Commissioner 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' for the draft DIS Code is the group consisting of providers of designated internet services, so far as those services are provided to end-users in Australia, as defined in s 135(2)(c).¹
8. The relevant 'online activity' for the draft DIS Code is providing a designated internet service, so far as the service is provided to end-users in Australia, as defined in s 134(c).
9. Clause 2(a) of the draft DIS Code stipulates its scope to apply to 'a provider of a designated internet service to the extent the service is provided to Australian end-users'. The head terms define 'Australian end-user' to mean an end-user who is ordinarily resident in Australia.
10. eSafety considers 'end-users in Australia' and 'Australian end-users' to be materially different concepts, despite the likely overlap, because the former term reflects an 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 an end-user who is 'ordinarily resident in Australia', the provisions identifying the section of industry and 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 is unlikely that the draft DIS 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)(c), or to the relevant online activity, described in s 134(c).

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 DIS 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 it unlikely that the draft DIS Code will meet the requirement under s 140(1)(d)(i) of the Act, because it does not provide appropriate community safeguards for Matters 1, 2, 4, 5 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 designated internet 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 DIS 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 DIS Code proposes minimum compliance measures (**MCMs**) 1 - 8 to deal with Matter 1.
16. eSafety considers that in order to provide appropriate community safeguards for Matter 1, the draft DIS Code would need to ensure that, at a minimum:
 - (a) end-user managed hosting services use systems, processes and technologies to detect and remove known child sexual abuse materials (**CSAM**); and
 - (b) Tier 1 DIS and end-user managed hosting services use systems, processes and/or technologies to detect and remove known pro-terror material/ Terrorist and Violent Extremist Content (**TVEC**); and
 - (c) Tier 1 DIS and end-user managed hosting services make ongoing investment in systems, processes and technologies in relation to class 1A material (including first generation CSAM).
17. eSafety does not agree with Industry Bodies' submission that the requirement to deploy technology to detect certain material should not extend to end-user managed hosting services due to potential user privacy concerns. Online file/photo storage sites have been found to be commonly used to facilitate dissemination of CSAM and TVEC.
18. Hash matching is the most common tool used to detect known CSAM and protect both the privacy of the general population (given the minimal risk of false positives²), but also of the child victims, whose privacy is repeatedly infringed when child sexual exploitation materials are shared online.
19. eSafety is aware of multiple examples of automated detection and human review processes to detect known CSAM deployed by some of the commonly used cloud-based file sharing services. eSafety's preliminary view is that a requirement for end-user managed hosting services to deploy such technologies to proactively detect known CSAM is reasonable and appropriate.
20. Further, eSafety considers that Tier 1 DIS and end-user managed hosting services could reasonably comply with a requirement to use systems, processes and/or technologies to proactively detect known TVEC. While this commitment would not require providers to use all three of systems and processes and technologies, eSafety notes that in practice, Tier 1 DIS and end-user managed hosting services 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).
21. There are multiple ways this broadly drafted requirement (which does not require the deployment of specific technology) could be met, including options appropriate for less well-resourced businesses.

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

- There is a mix of proprietary and open-source tools that are widely used (we note over 200 organisations use PhotoDNA).
- DIS 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.
- Alternatively, DIS 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.
- Service 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.

22. eSafety's current view is that it is not reasonable or appropriate to curtail the ongoing investment requirement in MCM 8 to *known CSAM*, due to the immensely harmful consequences associated with the creation, distribution and dissemination of first generation CSAM. Technologies and processes aimed at detecting first generation CSAM are increasingly being developed and also deployed on a range of services. eSafety considers that commitments by Tier 1 DIS and end-user managed hosting services to invest in the development of systems, processes and technologies is critical in order to provide appropriate community safeguards.

23. The commitments in the draft DIS Code also 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 some of the leading technology companies since 2020 including Dropbox, Mega, Apple, Google, Microsoft. 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, and 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 **new** child sexual abuse material via their platforms and services, and to consider where existing measures can go further to improve and invest in innovative tools and solutions (e.g. Principle 2).

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

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 detect and prevent access or exposure to, distribution of, and online storage of class 1B material.

24. The draft DIS Code proposes MCMs 9 - 12 to deal with Matter 2. MCM 10 stipulates that Tier 1 and Tier 2 DIS and end-user managed hosting services must implement appropriate systems and processes that enable the provider to take appropriate enforcement action for breach of its policies, and includes examples of appropriate processes.
25. eSafety has concerns that the lack of an explicit requirement to adhere to and enforce their policies will undermine the effectiveness of MCM 10, as well as making it potentially unenforceable from a compliance perspective. This is because DIS providers could demonstrate compliance with MCM 10 by publishing and maintaining such policies without taking action to enforce the policies.
26. eSafety notes that requiring DIS providers to apply or enforce their own policies does not remove service providers' ability to exercise discretion. Nor does it mean the service provider would be required to take certain action in all circumstances (such as terminating the provision of a service). Service providers have the flexibility to design and implement their policies to allow appropriate and proportionate responses to potential breach scenarios.
27. Further, as it is currently drafted, MCM 10(b)(i) appears to suggest that the standard operating procedures should require an end-user managed hosting service to refer reporters of class 1B materials to eSafety resources at first instance. As previously communicated to Industry Bodies, eSafety suggests all DIS providers respond to reports of class 1A and 1B material under their complaint mechanism before referring unresolved complaints to eSafety.

Matter 4

*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 **the hosting** of class 1A material and class 1B material in Australia.*

28. The draft DIS Code proposes MCMs 13 and 14 to deal with Matter 4.
29. eSafety has similar concerns as those raised in relation to Matter 3 with the drafting of these MCMs. eSafety considers that the absence of a clear commitment to apply or enforce acceptable use policies and terms of use agreements is likely to impact on the effectiveness and enforceability of MCMs 13 and 14.
30. Having regard to the measures proposed for Matter 1 and Matter 2 and the concerns set out above, eSafety's preliminary view is that in order for the draft DIS Code to provide appropriate community safeguards in relation to Matter 4, it would need to ensure:
 - it contains the steps in paragraph 16 above (which are also necessary in order to provide appropriate community safeguards in relation to Matters 1 and 2); and

- greater clarity in MCMs 13 and 14 to include an obligation to apply and enforce policies and terms of use agreements.

Matter 5

Measures directed towards achieving the objective of ensuring that industry participants have effective and scalable policies and procedures in place to facilitate consultation, cooperation and collaboration with other industry participants in respect of the removal, disruption and/or restriction of class 1A material and class 1B material, as well as accounts associated with this material.

31. The draft DIS Code proposes an optional measure to deal with this matter, which encourages DIS providers to adopt a range of example measures to support industry collaboration.
32. eSafety recognises the diverse range of services covered under the DIS Code and the potential practical difficulties in requiring all Tier 1 or 2 DIS providers to make this a minimum compliance measure. However, eSafety considers that end-user managed hosting services are a category of DIS providers where collaboration is reasonable and appropriate. This could take place, by example, via an annual industry forum, information sharing with eSafety, contribution to cross-sector online safety groups and/or supporting research and innovation. Proactive engagement within and across industry will complement the other compliance measures and help address displacement effects where bad actors find shelter in smaller or less mainstream platforms to host and disseminate harmful content.
33. eSafety suggests revising the measure to be a mandatory obligation for end-user managed hosting service.

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.

34. The draft DIS Code proposes MCMs 31 - 34 to deal with this matter with the reporting obligations varying for different category of DIS providers.
35. Under MCMs 32 and 33, Tier 2 DIS and end-user managed hosting providers must submit code compliance report within 6 months of receiving a request from eSafety, 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 report would be due to eSafety until 18 months after registration at the earliest.
36. eSafety has concerns that the timeframe for responding to requests for reports under MCMs 32 and 33 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 DIS Code. Without an effective review process, the capability of the DIS Code to provide appropriate community safeguards may be compromised.

37. eSafety's preliminary view is that the proposed 6 months' response timeframe in MCMs 32 and 33 is likely to prevent the measures from 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

38. 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.

39. eSafety has identified provisions in the head terms and draft DIS Code 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 it 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 DIS Code, the demographics of the actual user base of a service is not listed as a factor in the risk assessment. eSafety considers the extent to which a DIS attracts a large number of child users to be relevant to the risk profile, particularly if a chat/messaging function that is not limited to private messages within the service is offered. Such services have a relatively high risk of exposure to online predators and the risk of unwanted contact and grooming. eSafety suggests that DIS providers be required to factor in the age of their actual users in order to ensure a more accurate evaluation of potential online risks that could be enabled or facilitated by the online platform or service.

- Noting that the draft DIS Code does not specify what weighting is given to each of the factors listed in clause 5(b), eSafety is also concerned that DIS providers may underestimate their risk level if application of the tiers and relative weighting of the factors 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 DIS providers are required to demonstrate that the compliance measures they have adopted are reasonable, it would be difficult for eSafety to critically assess risk profile assigned by the DIS provider to the online activity if those risk factors are open to broad interpretation and the risk profile adopted does not accurately reflect the risk of harm.

Next steps

40. 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 DIS Code, which 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) a commitment by end-user managed hosting services to use systems, processes and technologies to detect and remove known CSAM;
 - (c) a commitment by Tier 1 DIS and end-user managed hosting services to use systems, processes and/or technologies to detect and remove known TVEC/pro-terror material;
 - (d) a commitment by Tier 1 DIS and end-user managed hosting services to make ongoing investment in systems, processes and technologies in relation to class 1A material (including first generation CSAM);
 - (e) a commitment by end-user managed hosting services to effectively respond to reports and complaints about class 1A and class 1B material (as opposed to referring to eSafety in the first instance);
 - (f) a commitment by Tier 1 and Tier 2 DIS and end-user managed hosting services to implement and enforce their terms of use and policies prohibiting class 1A materials;
 - (g) where the draft DIS 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;
 - (h) ambiguities and inconsistencies that could undermine the integrity and enforceability of the draft DIS Code should be resolved, and further guidance provided in the areas identified by eSafety in paragraph 39 above.
41. If Industry Bodies decide not to submit an amended code but wish to provide further information, the information should clearly explain how the existing MCMs will provide appropriate community safeguards despite the express concerns identified above.



42. 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.