19 January 2024

Executive Manager, Industry Regulation and Legal Services
Office of the eSafety Commissioner
PO Box Q500, Queen Victoria Building NSW 1230

BSA Comments on Australia's Draft Online Safety Industry Standards for Designated Internet Services and Relevant Electronic Services

BSA | The Software Alliance (**BSA**)[1] is grateful for the opportunity to provide the following comments and recommendations to Australia's eSafety Commissioner regarding the draft Online Safety Industry Standards for Designated Internet Services (**DIS**)[2] and Relevant Electronic Services (**RES**).[3]

BSA was part of the Steering Group of Industry Associations that worked to develop Industry Codes of Conduct, including the proposed Codes for DIS[4] and RES,[5] pursuant to Division 7 of Australia's Online Safety Act.[6] Although the eSafety Commissioner determined not to register the industry proposed DIS and RES Codes, we appreciate the Commissioner's continued effort to take into consideration the views and recommendations of affected stakeholders, including BSA and our members.

---

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. Follow BSA at @BSAnews.

BSA's members include: *Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.*

[2] *Online Safety (Designated Internet Services— Class 1A and Class 1B Material) Industry Standard 2024* at https://www.esafety.gov.au/sites/default/files/2023-11/Draft%20Online%20Safety%20%28Designated%20Internet%20Services-Class%201A%20and%20Class%201B%20Material%29%20Industry%20Standard%202024.pdf

[3] *Online Safety (Relevant Electronic Services— Class 1A and Class 1B Material) Industry Standard 2024* at https://www.esafety.gov.au/sites/default/files/2023-11/Draft%20Online%20Safety%20%28Relevant%20Electronic%20Services%20-%20Class%201A%20and%20Class%201B%20Material%29%20Industry%20Standard%202024%20_0.pdf

[4] *Schedule 3 – Designated Internet Services Online Safety Code (Class 1A and Class 1B Material)* at https://onlinesafety.org.au/wp-content/uploads/2023/04/230331_3_DIS-Schedule_FINAL_clean.pdf

[5] *Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material)* at https://onlinesafety.org.au/wp-content/uploads/2023/04/230331_2_RES-Schedule_FINAL_clean.pdf

[6] *Online Safety Act 2021, No. 76, 2021* at https://www.legislation.gov.au/Details/C2021A00076

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

BSA supports efforts by the eSafety Commissioner and others to mitigate the harm caused by unlawful or harmful online material, including child sexual exploitative material (**CSEM**) and pro-terror content. Many BSA members are at the forefront of voluntarily designing mechanisms to detect, remove, and disrupt unlawful and harmful content from their systems where practicable and in line with relevant laws and contractual obligations.

While the intentions underpinning the draft DIS and RES Standards are admirable, we are concerned that the proposed obligations will put undue burdens on BSA members' products and services, many of which represent relatively low risk of disseminating harmful content to the public while providing cutting edge digital solutions for enterprises and end-users in Australia in terms of functionality, security, and privacy protections. Such services are important for organisations of all kinds and sizes, securely and effectively underpinning innovation, economic growth, and job creation in Australia.[7]

Our main concerns with the draft DIS and RES standards, discussed in more detail below, include:

- **The introduction of completely new categories of DIS related to machine learning and artificial intelligence (AI).** While there may be a role for imposing binding rules on rapidly evolving AI-related services to address high-risk uses, it is premature to jump ahead of the substantial domestic and international deliberations around these matters through these online safety standards. This is particularly true when a broader government agenda on AI regulation is under development.[8]
- **The unwarranted expansion of obligations appropriate to high-risk services to lower risk enterprise DIS and end-user managed hosting services (EUMHS).** Many BSA members offer services that may fall into the categories of enterprise DIS or EUMHS. These companies already are making substantial investments, voluntarily, to address the issue of harmful online content on their services. Imposing strict obligations, detailed instructions on investments and contractual arrangements, requirements for proactive detection of certain content types, and onerous compliance and reporting obligations will do little to address the real sources of online harm in Australia and will make services like enterprise solutions and secure and convenient online storage more costly or less available in Australia.
- **The inclusion of unnecessary variations from the Online Safety Codes, including those already registered by the eSafety Commissioner.** By failing to align the draft Standards more fully with the registered Codes and their "Head Terms", service providers, users, and the eSafety Commissioner will struggle to interpret the online safety commitments required by the Codes and putative Standards in a coherent manner.

Premature Inclusion of Machine Learning and AI Within the Scope of the Draft DIS Standard

We are very concerned that the eSafety Commissioner, after years of close consultation with industry representatives including BSA, has proposed without any meaningful discussion to create two entirely new categories of DIS: 1) high impact generative AI DIS; and 2) machine learning model platform services. Further, the draft DIS Standard explicitly includes additional obligations for "providers of enterprise DIS" which "provide(s) pre-trained machine learning models for integration into a service deployed or to be deployed by an enterprise customer" (see DIS Standard Definitions). The impact of

[7] *How Enterprise Software Empowers Businesses in a Data-Driven Economy* at https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf, see page 2.

[8] *Safe and Responsible AI in Australia Discussion Paper, June 2023* at https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/Safe-and-responsible-AI-in-Australia-discussion-paper.pdf. See also *BSA Comments on Supporting Safe and Responsible Artificial Intelligence in Australia, 26 July 2023* at https://www.bsa.org/files/policy-filings/07262023safeai.pdf

these changes is likely to be very broad and would disrupt the deliberative process that the Australian Government is undertaking to address AI-related policy issues more broadly.

Several elements of the proposal could create substantial mandatory regulatory requirements on many generative large language models at a time when the Australian Government and many others are engaging in thorough and deliberative processes to consider how best to identify and mitigate risks from AI, including those related to harmful content. The draft DIS Standard's definition of "high impact generative AI" appears very broad. The general nature of the concept of "high impact" includes not only "harmful" content, but lawful and (in some contexts) acceptable content (e.g., age-restricted) that may only be deemed harmful to children or in certain other specific circumstances. In addition, generative AI may be deemed "high impact" if it is "***reasonably*** foreseeable that the service ***could*** be used to generate synthetic high-impact material" (DIS Standard Definitions, emphasis added).

As with all tools, machine learning algorithms and generative artificial intelligence (**AI**) systems have risks, and these risks may extend to the generation and dissemination of harmful online content in certain circumstances. The Australian Government and many others so far have proceeded cautiously and deliberately in developing comprehensive rulemaking to identify and mitigate risks associated with AI. Even the European Union, which may be the furthest along in terms of establishing a comprehensive legislative framework to address high-risk applications of AI systems, has deliberated this position carefully over several years and will provide a two year transition period from when the EU AI Act comes into law before it will be enforced.

When thinking about any kind of AI regulation, it is important to consider the suitability of different responsibilities for different actors, based on their position in managing different aspects of AI technology. For example, enterprise DIS making third-party AI applications available to other enterprises are not in a position to influence the AI model's development or its use.

BSA firmly supports appropriately crafted rulemaking related to high-risk uses of AI.[9] However, there has been very little consultation and discussion with relevant stakeholders regarding the role of AI in generating harmful content in Australia and the appropriate means by which to address this risk.

Therefore, we urge the eSafety Commissioner to remove all references to AI from the draft DIS Standard and instead encourage a mechanism to engage in a comprehensive discussion with relevant stakeholders, including across the Australian Government, to determine an appropriate path forward to address the existing and potential risks of harmful content generated or disseminated by AI systems.

In addition, any proposals to address AI-related on-line harms should be conducted in the context of the Australian Government's overarching approach (whether recommendatory through the development of voluntary guidelines, or mandatory through a legislative process) to identifying and addressing risks presented by AI.

Expansion of Obligations Designed for High-Risk DIS to Enterprise DIS and End-User Managed Hosting Services (EUMHS)

In the draft DIS Standard, the eSafety Commissioner proposes to require enterprise DIS and EUMHS to adopt many of the same obligations as Tier 1 DIS. Tier 1 DIS are, by definition, DIS with a high risk that class 1A material or class 1B material will be accessed or generated by, or distributed to, end-users in Australia using the service, or will be stored on the service.

[9] *BSA Welcomes AI Act Agreement, Urges Balanced Implementation, 8 December 2023* at https://www.bsa.org/news-events/news/bsa-welcomes-ai-act-agreement-urges-balanced-implementation, *BSA Written Testimony on White House Policy on AI, 6 December 2023* at https://www.bsa.org/files/policy-filings/12062023writtestwhitehouseaipolicy.pdf, *BSA House Energy and Commerce Testimony, 18 October 2023* at https://www.bsa.org/files/policy-filings/bsa_house_energy_and_commerce_testimony-final.pdf, See also *BSA's AI Resource Center* at https://ai.bsa.org/

While it is *possible* for end-users to store, distribute, or provide access to this material on EUMHS, they are not typically at a "high risk" to do so. Such services' primary purpose (and function) is to provide affordable, secure, and easily accessible file storage for end-users.

In the case of enterprise DIS, an extremely broad category of entities and services, these services' primary purpose (and function) is to provide productivity and security enhancing services to enterprise customers.[10] As a result, their services tend to pose a far lower risk of creating, storing, or transmitting harmful content. In addition, there is often no direct relationship with the end-user and, therefore, no ability for the enterprise DIS provider to moderate specific instances of content.[11]

It is therefore practically and technically infeasible for enterprise DIS to interfere with the end-users of their enterprise customers and the draft Standards should not impose obligations on such entities to do so.

CSEM and Pro-Terror Material

Section 15 imposes obligations on EUMHS and AI-related services to notify authorities and organisations about not just known child sexual abuse material (**CSAM**) but all CSEM and pro-terror material, including new material. We have argued that AI-related services should be excluded from the scope of the DIS Standard. Given the lower risk profile of most EUMHS compared with other online services, technical limitations, and the reasonable privacy expectations customers have of such services that the provider is not reviewing or inspecting their data, ***including EUMHS in these obligations is impractical and will impose costs and limitations on providers and end-users in Australia that are not proportionate to the likely harms.***

Section 15 requires a provider (including providers of EUMHS and AI-related categories) to notify authorities (Section 15(2)), "an organisation of a kind referred to…" (Section 15(3)), and "an organisation that verifies material as pro-terror" (Section 15(4)) when it "identifies" certain kinds of content related to CSEM and pro-terror material.

First, the use of the term "identifies" pre-supposes some mechanism the provider itself possesses to identify such data, including not only known CSAM material, but also new CSAM and CSEM and pro-terror material. Many EUMHS are incapable of doing so for technical reasons, the contractual commitments they undertake with their customers against reviewing customer data, and other limitations. To the extent EUMHS providers must notify, ***we recommend using the term "becomes aware of" — as it may be that a primary means for a provider to become aware of such material on their system is by receiving information via a third party.***

Second, regarding notifying organisations about pro-terror material, it is unclear which organisations are in place and have the authority to act as a centralised international clearinghouse of such content. The only shared hash list of terrorist content of which we are aware is that maintained by the Global Internet Forum to Counter Terrorism (**GIFCT**) and not all BSA member companies have access to this list. Furthermore, the GIFCT has a strict process for onboarding new members to ensure fundamental rights are upheld in the organisation.[12] It is inappropriate for Australia's Online Safety Standards for DIS and RES to place pressure on both the GIFCT and other companies to be part of this process.

Third, to a much greater extent than CSAM and even CSEM, whether content should be deemed pro-terror content frequently depends on context. Unlike CSAM, there are a variety of reasons why an

---

[10] *How Enterprise Software Empowers Businesses in a Data-Driven Economy* at https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf

[11] See *BSA Response to the Online Safety Bill 2020 Consultation, 12 February, 2021* at https://www.bsa.org/files/policy-filings/02122021ausonlinesafety.pdf, *BSA Comments to the Online Safety Bill 2021 Committee Inquiry, 2 March 2021* at https://www.bsa.org/files/policy-filings/03022021ausonlinesafetycmte.pdf, and *BSA Comments on the draft Online Safety (Basic Online Safety Expectations) Determination 2021, 12 November, 2021* at https://www.bsa.org/files/policy-filings/11122021bosecmts.pdf

[12] *Global Internet Forum to Counter Terrorism (GIFCT), Membership* at https://gifct.org/membership/

end-user in Australia may have a legitimate reason for possessing content that may be deemed "pro-terror" in other contexts. Additionally, the harm caused by such content does not stem from its generation and consumption as much as from when this content is shared with a larger audience, which in the case of private EUMHS is relatively uncommon. When kept privately and not used in a manner that causes harm to other end-users, such content might not be deemed "pro-terror". This is particularly poignant today given the current conflict in the Middle East where there is very legitimate debate about what constitutes terrorism and therefore "pro-terror" material with significant disagreements between legitimate international bodies. It is unreasonable to request or require EUMHS providers to inspect customer data not only for possible matches to hash lists, which may not be available to all such providers, but also inspect customers data for other "contextual' signals to determine the actual nature and intent behind possession of such content.

While it may be appropriate to request and require EUMHS providers to notify relevant authorities and organisations when they become aware of a user account possessing known CSAM or strong evidence of CSEM, ***we recommend that EUMHS (and AI-related services if retained within the scope of the DIS Standard) not be required to report alleged pro-terror content for the reasons we outline above.***

Similarly, Section 17 requires EUMHS and AI-related services to take certain actions once the provider "becomes aware" there has been a breach of the providers' acceptable use policies or community standards involving not only known CSAM, but all CSEM (including new content) and pro-terror content.

Given there is ambiguity in the obligations related to this section, ***we recommend making clear that the requirement in Section 17(2) to "remove instances of CSEM and pro-terror materials identified" refers to specific content associated with a specific account holder.***

Regarding the termination of a user's account, it may be difficult for an EUMHS provider to assess whether an end-user has the "intention to cause harm". Also, it may not be appropriate to immediately terminate an account which is being used by an Australian child if the account holder was unaware of this activity.

We recommend removing Section 17(2)(d)(i) from the Standard and adjusting Section 17(2)(d)(ii) to indicate that termination is warranted if the account holder is not able or willing to prevent a child from using the account. This is consistent with Section 17(2)(d)(iii) which requires account termination if the account holder has "repeatedly breached the terms and conditions…"

Detecting and Removing Known CSAM and Known Pro-Terror Material

Section 21 and 22 requires providers of EUMHS and high-impact generative AI DIS to "implement systems, processes and technologies" to detect known CSAM and known pro-terror material, respectively.

The draft Standard helpfully acknowledges that it may not be technically feasible to comply with all the requirements of Section 21 and 22. ***However, we strongly recommend including, in its entirety, Section 6 of the Industry Code Head Terms, which the Commissioner approved when registering the Industry Codes, in both the DIS and RES standards.*** Otherwise, the greater certainty and clarity regarding circumstances in which higher risk services subject to some of the Industry Codes are to interpret their obligations will not apply to lower risk EUMHS and other services covered by the Standards. This is an unfair and unreasonable outcome of the development of Industry Standards and adds significant confusion to the overall set of codes and standards that will eventually be in force.

In addition, and as described above, imposing the obligation to "implement systems, processes and technologies" to detect known known pro-terror material under Section 22 on EUMHS and high-impact generative AI DIS raises the same problems described above for Section 15 and 17. Unlike

known CSAM material, the harm caused by the possession and distribution of pro-terror material is far more context-specific and generally only occurs if material is shared. ***Therefore, we recommend removing EUMHS and high-impact generative AI DIS (if retained in the Standards against our recommendation) from Section 22.***

Disrupting and Deterring CSEM and Pro-Terror Material

Section 23 applies to EUMHS, enterprise DIS, and AI-related services, in addition to Tier 1 DIS. As with the Sections described above, ***it is neither reasonable nor feasible to apply obligations associated with the services at high risk of online harms to lower risk services like EUMHS, enterprise DIS, and AI-related services.***

Furthermore, because of the nature of the services, in which end-users of EUMHS and enterprise customers of enterprise DIS reasonably expect a high level of privacy and data protection (in addition to seamless functionality and the highest levels of cybersecurity), the services frequently are not technically engineered nor contractually offered in a manner that enables the service provider to view and inspect content.

We have already described the challenges of determining known and unknown "pro-terror material" for EUMHS. When a service is prohibited technically, legally, or contractually from inspecting end-user data, ***it is similarly impractical to effectively "disrupt and deter" end-users from using these services regarding new CSEM material or pro-terror material.***

The inclusion of enterprise DIS in this specific obligation also is very problematic. Enterprises that provide services to other enterprises normally have no means to interact with end-user content generation and use. Similarly, enterprise DIS have technical, legal, and contractual obligations to not inspect their enterprise customer data. We recommend that enterprise DIS be removed entirely from this obligation.

With respect to AI-related services, an additional consideration is that there may be an extent to which AI systems require training on certain unlawful or harmful material to understand the types of material it must avoid generating and the types of prompts it needs to ignore or handle differently. Therefore, entirely "clean" training data may reduce the effectiveness of such tools and reduce the likelihood they operate with precision and nuance. The requirement outlined in section 23(4) could have the inadvertent effect of making generative AI less capable of identifying and preventing the generation of certain high-risk material including CSAM.

Consistent with our overarching recommendation to remove AI-related services in their entirety, including enterprise DIS offering services which provide pre-trained AI or machine learning models for integration into their customers' deployed services, from the scope of the DIS Standards, we urge the eSafety Commissioner to remove Sections 23(3) and 23(4) from the DIS Standards.

Resources

Section 20 requires EUMHS and AI-related services to maintain "sufficient" personnel to meet the requirements of the Standard. EUMHS has a much lower risk of harm than other services, including Tier 1 DIS and services addressed in other Industry Codes, particularly as content often is not shared outside EUMHS and is unlikely to become viral if it is, which is why we did not include this obligation for EUMHS in the industry association developed DIS Code. If this obligation is retained for EUMHS and AI-related services, ***it is very important for the eSafety Commissioner to 1) review the draft Standards in their entirety to ensure that the Commissioner is not inadvertently imposing unreasonable compliance burdens on EUMHS providers and 2) ensure that interpretation of "sufficient personnel" to comply with the standards is proportionate and understandably less than that required by higher risk service providers.***

Section 23 of the draft DIS Standard and Section 24 of the Draft RES Standard require providers to establish and implement, for the calendar year, a program of investment and development activities in respect of systems, processes, and technologies focused on disrupting and deterring CSEM and pro-terror material, including first-generation material. These programs can be requested by the eSafety Commissioner. This requirement may be quite burdensome and not necessarily an effective use of limited resources. First, it is not clear that imposing such an obligation on all service providers will prove more effective than the dissemination of innovative solutions from industry leaders to partners and competitors. ***Obligating such investments is an inappropriate extension of the Commissioner's powers into the online marketplace and may not achieve the intended results.***

Furthermore, solutions to identify first generation or new material are not as reliable as solutions such as hash matching for identifying known harmful material, and humans must be in the review loop to ensure false positives are not reported with an impact on user rights. A requirement to detect new material therefore presents a significant risk to end-user privacy, particularly in a situation where end-users expect content will remain secure and private. ***Therefore, requirements to invest in systems, processes, and technologies to detect and identify new CSEM material (in addition to known CSAM) and pro-terror material may present unacceptable risks to privacy and the reasonable expectations of enterprise customers and users of EUHMHS that their data will not be viewed or inspected by the service provider.***

Unnecessary Differences from the Registered Industry Codes and the Accompanying Head Terms

On 16 June 2023, the eSafety Commissioner published five Industry Codes AND the accompanying "Head Terms" (subsequently amended on 12 September 2023).[13] The Head Terms provide common terms, concepts, and interpretations for the registered Industry Codes.

As noted above, with respect to "technical feasibility" and the concepts and guidance provided in Section 6 of the Head Terms, the fact that the Head Term concepts have not been consistently included in the draft DIS and RES Standards will create unnecessary challenges for compliance with the Standards and may result in an unfair and disproportionate burden imposed on DIS and RES, even when many applications of such services may be lower risk when compared to some of the industry sections for which Industry Codes have been registered.

Functionality vs Purpose

An important example of this is the difference between how a service provider is expected to determine whether a particular service will be covered by the Codes or Standards. In the Industry Code Head Terms, a service provider is to determine "the industry standard that is most closely aligned with the ***predominant purpose*** of the single electronic service" (emphasis added).[14] This contrasts with the draft Standards' requirement that service providers determine the "***predominant functionality***" of the service.[15]

---

[13] *Register of industry codes and industry standards for online safety* at https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards.

[14] *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms, 12 September 2023*, page 4 of 29 "Identifying the applicable code or standard" at https://www.esafety.gov.au/sites/default/files/2023-09/Consolidated-Industry-Codes-of-Practice-Head-Terms-12-September-23.pdf.

[15] *Online Safety (Designated Internet Services—Class 1A and Class 1B Material) Industry Standard 2024* at https://www.esafety.gov.au/sites/default/files/2023-11/Draft%20Online%20Safety%20%28Designated%20Internet%20Services-Class%201A%20and%20Class%201B%20Material%29%20Industry%20Standard%202024.pdf and *Online Safety (Relevant Electronic Services— Class 1A and Class 1B Material) Industry Standard 2024* at https://www.esafety.gov.au/sites/default/files/2023-11/Draft%20Online%20Safety%20%28Relevant%20Electronic%20Services%20-%20Class%201A%20and%20Class%201B%20Material%29%20Industry%20Standard%202024%20_0.pdf, Sections 5.

While it is not clear whether or to what extent there is a difference between the concepts of "purpose" vs. "functionality" when modified by the term "predominant", it is unhelpful to have services determined to fall within the scope of the DIS or RES Standards to be assessed by a different standard than services falling under one of the six industry sections subject to the Industry Codes. Strictly speaking, functionality is not the best measure of the risk of online harm. Many services have a variety of "functions", such as communications, storage, etc., but if the purpose of the service is such that these functional features are not presented to end-users or used by end-users in a way that is likely to result in the creation, communication, dissemination, or storage of harmful online content, determining a services category based on "functionality" may result in the treatment of service as if it presents a higher risk than what the service's purpose or typical use would warrant.

Therefore, ***we recommend that the draft DIS and RES standards incorporate the Industry Codes' Head Terms concept of determining the appropriate Code or Standard based on predominant purpose instead of predominant functionality***.

Other Observations and Recommendations

Applicability of Risk Assessments

Section 8 of both the draft DIS and RES Standards describes the requirements for a DIS or RES provider to conduct risk assessments. However, Section 8(6) states that several categories, including EUMHS, enterprise DIS, the AI categories for DIS, and enterprise RES and others for RES are exempt from Section 8(1) (the obligation to carry out a risk assessment) and Section 8(4) (the requirement NOT to start providing a DIS or RES unless the provider has conducted a risk assessment).

It is, therefore, unclear how Section 8(2) (the requirement to conduct a risk assessment within 6 months of the draft DIS or RES Standard coming into effect), Section 8(3) (the exemption from completing a risk assessment within 6 months of the draft DIS or RES Standard coming into effect if a risk assessment was already completed with 6 months prior), and Section 8(5) (the prohibition of making a material change before conducting a risk assessment) would apply to the services described in Section 8(6)). In the case of Section 8(5), we understand that even a material change to a service, but one that does not change a service from, for example, an enterprise DIS, enterprise RES, or EUMHS, would not require a risk assessment because enterprise DIS, enterprise RES, and EUMHS are exempt from this requirement. ***We recommend that Section 8(6) state the subsections (2), (3), and (5), in addition to subsections (1) and (4), do not apply to the listed categories.***

We also recommend making clear that Section 34 for DIS and Section 33 for RES (which allows the Commissioner to request information about the most recent risk assessment) also does not apply to enterprise DIS, enterprise RES, EUMHS, the AI-related categories, and the other categories listed in Sections 8(6) for the same reasons.

Redundancy Between Terms of Use and Statement of Community Standards

Section 32 of the Draft DIS Standard and Section 31 of the Draft RES Standard requires service providers to publish "the terms of use for the service, including provisions relating to acceptable use policies" AND "a statement setting out the community standards applicable to the service". It is not clear to us what the difference between these two concepts are and whether the terms of use or "acceptable use" policies that are commonly in use among BSA members could also act as the "statement" regarding community standards and therefore avoid the need for an Australia-specific and duplicative document. ***We recommend that DIS Section 32(2) and RES Section 31(2) replace "and" between sub-clauses (a) and (b) with "or" or otherwise make clear that if the required information is included in the terms of service and/or acceptable use policies, a separate "statement of community standards" is not required.***

Missing Sub-section 6(2)

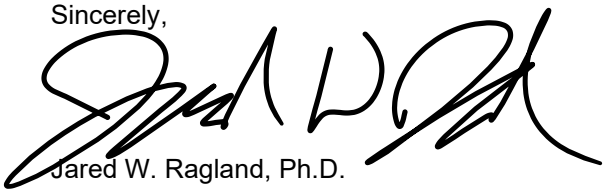
We note that there appears to be no Section 6(2) in the draft DIS Standard. Section 6(1) lays out general definitions and Section 6(3) describes requirements for a "pre-assessment".

Conclusion

We thank the eSafety Commissioner for the positive consideration of these observations and recommendations. We hope that our recommendations will be implemented in the final versions of the DIS and RES standards to ensure effective and proportionate actions to be taken by relevant online service providers to identify and minimize the risks of online harms for Australians. As a member of the Industry Steering Group that worked to develop the Online Safety Industry Codes, we understand the complexity and challenges of identifying actions to be taken by service providers that are effective and practical, are proportionate to the risks that various services present with respect to online harm, and reflect the enormous benefit that many services provide to Australian end-users, especially those supporting enterprises and other organisations in Australia to promote innovation, economic growth, and job creation. It is also critical that the Standards and Codes reflect the reasonable expectations of enterprise customers and end-users in Australia for privacy and data security.

We look forward to continuing our work with the eSafety Commissioner and her office and other relevant stakeholders to continuously enhance protections against online harms while ensuring that Australian's have affordable access to the cutting edge software-enabled services that enhance productivity, security, and the goals of digital transformation that BSA members offer globally.

Sincerely,



Jared W. Ragland, Ph.D.
Senior Director, Policy – APAC
BSA | The Software Alliance