Fact sheet: Post consultation changes to the Designated Internet Services Standard

June 2024

21 June 2024

Following consultation with industry, civil society organisations and other stakeholders the eSafety Commissioner (eSafety) has registered the Online Safety (Designated Internet Services – Class 1A and Class 1B Material) Industry Standard 2024 (known as the 'DIS Standard').

The DIS Standard minimises and prevents harms associated with access and exposure to the most harmful forms of online material on these services. It covers two types of class 1 material that are associated with serious harms. These are:

- class 1A material, such as child sexual exploitation material (including child sexual abuse material) and pro-terror material
- class 1B material, such as crime and violence material and drug related material.

This fact sheet outlines some of the key changes made to the scope and obligations of the DIS Standard following consultation. More information about the consultation – including submissions and summaries of the roundtables – can be found at: eSafety.gov.au/industry/codes/standards-consultation.

Key changes to the scope and services covered by the DIS Standard

Section (current reference)	Details of change
5 Application of this industry standard **6 General definitions - use of predominant purpose**	**Change to test.** The test for determining whether the DIS Standard or another industry Standard or code applies to a service is now the service's predominant purpose, instead of its functionality. This test is also used in the definitions of different DIS categories. (This change takes into account feedback that the predominant purpose is clearer for service providers to identify the applicable standard or code and the most relevant category in the DIS Standard.)
6 General Definitions – high impact generative AI DIS	**Definition amended.** To clarify that where a service deploys controls which make it unlikely that it could be used to generate synthetic high impact material (X18+ or RC), the service will not be defined as a high impact generative AI DIS.
6 General definitions – Model distribution platform	**Category renamed and definition amended.** The 'machine learning model platform service' category has been renamed the 'model distribution platform' category. In addition, the definition of a model distribution platform has been amended to clarify that only services which host third party machine learning models uploaded by end-users are in scope.
6 General definitions – enterprise DIS	**Risk profile changed.** The risk profile of an enterprise DIS is now deemed to be Tier 3 (the lowest risk). The obligations specific to an enterprise DIS have also been removed, so only the obligations for Tier 3 services now apply.
Technical feasibility definition	**Removal of a section and amendment to approach.** The former Section 7, which included the technical feasibility definition, has been removed. Consistent with the approach in other legislation, technical feasibility is now undefined in the DIS Standard and will maintain its 'ordinary meaning' under the law.

Key changes to the obligations applying to DIS categories

Section (current reference)	Details of change
13 Having terms of use addressing class 1A and 1B material **22 Disrupting and deterring end-users from using the service to solicit, generate, access, distribute, or store child sexual exploitation material and pro-terror material** **36 Giving eSafety a report which details a service's compliance with the DIS Standard**	**Sections no longer apply to a service type and upstream obligations limited.** These sections no longer apply to an enterprise DIS. (This change is based on feedback indicating that these measures were disproportionate to the risk of these services.) In addition, the change limits obligations on upstream generative AI model developers, which are captured as enterprise DIS, while the eco-system for generative AI services develops and broader regulation is considered.
19 Resourcing trust and safety functions through internal reporting arrangements that ensure compliance and can supervise online safety of the service **23 Implementing a development program investing in and developing systems, processes and technologies which enhance online safety** **24 Carrying out an assessment of the design features which could be incorporated into the service to minimise risks, and incorporating those features and settings**	**Sections no longer apply to a service type.** These sections no longer apply to model distribution platforms. (This change is based on feedback that some obligations were disproportionate and infeasible.)

25 Having in place policies and procedures which ensure a service responds to communications from eSafety and refers unresolved complaints to eSafety **26 Giving information on a service to end-users in Australia about eSafety including how to refer matters to eSafety**	
34 Notifying eSafety of new features of a service which would significantly increase the risk of class 1A and 1B material	**Section applies to further service types.** Tier 2 services and end-user managed hosting services have been added to Section 34. (This is to provide greater transparency around the changing risk levels of services.)

Changes to the DIS Standard's obligations

Section (current reference)	Consultation draft obligations	Details of change
20 Detecting and removing known child sexual abuse material **21 Detecting and removing known pro-terror material**	A service provider was not required to use a system, process or technology where it was not technically feasible for the provider to do so, under former sections 21(3) and 22(3).	**Amendment to section numbering and addition of further exceptions.** Former Sections 21(3) and 22(3) are now Sections 20(3) and 21(5) respectively. The obligation remains the same, but a service provider is also not required to implement a process, system or technology under any of these circumstances: • If it is not reasonably practicable to do so. This change is based on feedback that technical feasibility alone was inadequate to encompass broader impediments that a service provider might encounter in implementing a technology, such as cost or business model limitations. However, those impediments alone would not be enough to demonstrate that something is not reasonably practicable – the extent of the challenges faced by service providers must be balanced against the severity of risks and harms to end-users. • If doing so would introduce a systemic weakness or vulnerability into the service. • If the service is end-to-end encrypted and doing so would build a new decryption capability into the service or render methods of encryption used in the service less effective. (This change is based on feedback that end-to-end encrypted services require an explicit reference).

		If any of these circumstances apply, a provider must take appropriate alternative action.
11 Determining what is appropriate **20 Detecting and removing known child sexual abuse material** **21 Detecting and removing known pro-terror material** **22 Disrupting and deterring child sexual exploitation material and pro-terror material**	'Appropriate' and 'appropriate action' were used in some obligations to ensure that services could comply in a way which was suitable to their circumstances and the potential harms.	**Amendment to section numbering and addition of a further consideration.** Former Section 12 has been changed to Section 11. In considering whether something is 'appropriate', Section 11 now includes a consideration of whether it is proportionate to the level of risk to the online safety of end-users in Australia. (This change incorporates feedback that some obligations were not proportionate or feasible for particular service providers.) In addition, the wording in Sections 20-22 has been amended to ensure that matters like proportionality are considered when providers implement 'appropriate' systems to: • detect and remove known child sexual abuse material and known pro-terror material (Sections 20-21) • disrupt and deter child sexual exploitation material and pro-terror material (Section 22).

13 Terms of use **15(4) Model distribution platforms responding to breaches of terms of use of child sexual abuse material and pro-terror material**	Services were required to have a 'terms of use' in place regarding class 1A and 1B material, and to take appropriate action to respond to breaches of their terms of use, under the former Section 14.	**Amendment to section numbering and addition of clarifying wording.** Former Section 14 is now Section 13. The obligation remains the same, but wording has been added at Section 13(4) to provide clarity that 'terms of use' has a commonly understood meaning and that a different name may be used by the service provider as long as it has the same contractual effect as 'terms of use' and incorporates the obligations for dealing with breaches set out in Sections 13(2) and 13(3). In addition, Sections 13(3) and 15(4) now make it clear that model distribution platforms, like other identified services, need to have and enforce their terms of use in relation to hosted models.
21 Detecting and removing known pro-terror material	Relevant services were required to detect and remove known pro-terror material stored on the service, or being accessed or distributed by the service.	**Addition of a clarifying subsection.** The obligation remains the same for all service types, but the addition of Section 21(10) clarifies the obligation for end-user managed hosting services. Specifically, the obligation for end-user managed hosting services to detect and remove known pro-terror material in inert spaces (where content is at rest) only applies if the provider suspects that the end-user is storing pro-terror material and the account has been accessed by multiple individuals. (This is to account for difficulties in detecting pro-terror material stored in inert environments.)
29 Additional rules for Tier 1 services reviewing end-user reports	A service provider was required to take appropriate action to respond promptly to reports made by end-users, and ensure that an end-user who makes a report was notified	**Addition of an obligation.** Section 29 now requires that where a Ter 1 service end-user requests a review of the outcome of a report

	promptly of the outcome of the report and able to request a review.	concerning class 1A or class 1B material: • the review must be conducted by a person other than the person who conducted the investigation into the initial report • the provider must take appropriate action to facilitate the review. (This has been changed to provide clarity on the process of reviewing reports, and to align with the RES Standard.)
33 Notifying changes to features and functions in relation to generating high impact material	Service providers were required, as soon as practicable, to notify eSafety when making a change that would significantly increase the risk of Class 1A and 1B material, under the former Section 36.	**Amendment to section numbering addition of a section.** Former Section 36 is now Section 34. Section 33 has been added, requiring providers to also notify eSafety when changing a feature or function that makes it significantly more likely to generate R18+, X18+ or RC material, which is high impact material. (This change was made to ensure that services are appropriately assessing their risk levels and identifying their DIS categories.)
36 Commissioner may require compliance reports	This section allowed eSafety to request a report that detailed how a provider complied with applicable obligations.	**Addition of detail to an obligation.** Section 36 has been amended so that compliance reports must include the number of complaints made to the provider about the provider's compliance with this industry standard during the reporting period. This gives eSafety oversight over the effectiveness of the standards, and aligns this element with the RES Standard.
36 Commissioner may require compliance reports	Under the former subsection 38(7)(a)(ii) the minimum step required of model distribution platforms was to report on the number of models made available through the service in all calendar years when it was reasonably foreseeable that the model could	**Addition of detail to an obligation.** Former Subsection 38(7)(a)(ii) is now Subsection 36(7)(a)(ii), which has been amended so that where a model distribution platform is required to provide a compliance report, it must include the number

	be used to generate child sexual abuse material or pro-terror material.	of models identified to be in breach of its terms of use in relation to child sexual exploitation material and pro-terror material. (This incorporates feedback that it is not feasible for these services to identify models where it is reasonably foreseeable that the model could be used to generate child sexual abuse material or pro-terror material.)