Australian Telecommunications Alliance

Setting The Standard.
Driving Progress.

AUSTRALIAN TELECOMMUNICATIONS ALLIANCE SUBMISSION

To: Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts

Re: *Online Safety Amendment (Digital Duty of Care) Bill 2026* and Consultation Paper

22 September 2026



TABLE OF CONTENTS

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE 3

2. INTRODUCTION 3

3. PRINCIPLES FOR A DUTY OF CARE 4

1. REASONABLY PRACTICABLE 4

2. BUSINESS AND ENTERPRISE SERVICES 5

4. APPS OR WEBSITES FOR THE MANAGEMENT OF C/CSP SERVICES 5

5. RESALE OF SERVICES AND EQUIPMENT 6

3. FEEDBACK FEATURES 6

6. RISK ASSESSMENTS 7

7. COMPLAINT AND DISPUTE PROCESS 8

8. DIGITAL DUTY OF CARE GUIDELINES 8

9. ENFORCEMENT AND PENALTIES 8

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE

1.1 The Australian Telecommunications Alliance (ATA) is the peak body of the Australian telecommunications industry. We are the trusted voice at the intersection of industry, government, regulators, and consumers. Through collaboration and leadership, we shape initiatives that grow the Australian telecommunications industry, enhance connectivity for all Australians, and foster the highest standards of business behaviour. For more details, visit www.austelco.org.au.

1.2 For questions on this submission, please contact Deputy CEO Christiane Gillespie-Jones, c.gillespiejones@austelco.org.au.

This is submission is provided on behalf of our carrier and carriage service provider (C/CSP) members. Individual members may make additional submissions.

2. INTRODUCTION

2.1 The ATA welcomes the opportunity to provide a submission to the Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts (Department) in response to the Exposure Draft of the *Online Safety Amendment (Digital Duty of Care) Bill 2026* (Bill) and associated Consultation Paper.

2.2 We thank the Department for the discussion that it recently facilitated. We base some of our comments on the information provided during that discussion.

2.3 The ATA supports the overall objective to protect Australians, especially the most vulnerable online participants and children, from harmful online content and to promote online safety more broadly.

2.4 In addition to member-specific initiatives to enhance user safety and promote online safety, and compliance with lawful requests to block online domains, our members comply with the requirements of the *Online Safety Act 2021* (OSA) and its subordinate instruments, i.e. the

a) Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) (Class 1 Codes),

b) Consolidated Industry Codes of Practice for the Online Industry (Class 1C and Class 2 Material) (Class 2 Codes),

c) Online Safety (Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024 (DIS Standard),

d) Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024 (RES Standard), and

e) Online Safety (Basic Online Safety Expectations) Determination 2022 (BOSE).

2.5 Given the limited consultation period and building on the feedback we previously provided in response to consultations on the Digital Duty of Care (DDOC), we confine our feedback to the most critical issues of the Exposure Draft. As requested, we will limit our comments on matters of policy to issues that we believe are relevant to the Exposure Draft itself or associated explanatory material and guidance.

3. PRINCIPLES FOR A DUTY OF CARE

3.1 In our view, the DDOC ought to operate as a duty on certain providers to ensure that they take steps/care to protect vulnerable online users from online harms, including by limiting access and distribution of harmful content.

3.2 We continue to hold the view that the DDOC ought not to be based on the overly broad scope of services of the OSA. Instead, at a minimum, all of the following threshold criteria ought to be satisfied to bring a service in scope for the DDOC:

a) Significant risk of harm emanating from access to and distribution of regulated (harmful) content through the service;

b) Visibility and editorial or other control over the content or its distribution; and

c) No legal prohibitions to obtain visibility of the content and/or to exert control over the content.

3.3 C/CSP members provide the following services that are currently in scope, or could be argued of being in scope, of the OSA:

a) SMS/MMS, i.e. 'traditional' texts and multimedia messages sent by users by means of a carriage service. (For iOS users, SMS appear as green messages.) Note that these services do not include other messaging services that are provided 'over the top' (OTT), such as WhatsApp or iMessage or other OTT Rich Communication Services (RCS). (For iOS users, iMessages appear as blue messages.);

b) Email services provided as part of a contract for carriage services, e.g. Optus Webmail or Bigpond. Note that these services do not include email services that run 'over the top' by means of a carriage service, e.g. they do not include gmail, Hotmail etc.;

c) Internet carriage services (ICS), i.e. access to and connectivity via the internet. Note that these services do not include any services that use internet connectivity to be delivered;

d) Certain business/enterprise services;

e) Certain apps or websites for the management of the C/CSP services; and

f) Resale of services (e.g. entertainment services) and equipment.

3.4 **The services that our members provide arguably do not satisfy the criteria of section 3.2 above. Therefore, we believe that the Minister ought to make use of the right to exempt services of low risk pursuant to section 25A(3)(a) of the Bill.**

3.5 Limiting the scope to the services of higher risk and capacity to limit harm would also align with the recent recommendations by the Productivity Commission to reduce regulatory burden and red tape.

3.6 We provide the following feedback in case no Ministerial exemption for C/CSP services is granted.

1. REASONABLY PRACTICABLE

3.7 Broadly speaking, the operation of the DDOC turns on whether measures or actions taken to enliven the DDOC are 'reasonably practicable' for regulated entities. This is especially the case for C/CSPs as, by and large, they do not have visibility and editorial or other control over content or its distribution and/or are constrained by legal prohibitions to obtain visibility of the content and/or to exert control over the content.

3.8 Therefore, it is imperative for C/CSPs to have the greatest possible certainty that their actions are considered

reasonably practicable and, therefore, they are compliant with the requirements of the DDOC that rely on regulated entities taking reasonably practicable action.

3.9 C/CSPs already comply with the requirements of the Class 1 and 2 Online Safety Codes and the Class 1 RES and DIS Standards, with Internet carriage services providers also complying with lawful requests to block domains.

3.10 Given the low risk of the services provided and the lack of visibility or editorial control over content, **we submit that C/CSPs will be deemed compliant with the reasonably practicable standard if they continue to fulfil the requirements of these instruments beyond the envisaged deregistration/revocation of those instruments. We submit that the Explanatory Memorandum to the Bill ought to clearly outline this approach.**

3.11 We understand from recent discussions with the Department that it is believed that C/CSPs continuing to comply with these requirements would be 'well placed' to be deemed compliant with the DDOC.

3.12 **We also seek confirmation that carriers purely acting in a wholesale capacity are out of scope for the DDOC.**

3.13 For providers operating at the intermediate communications layer, taking reasonably practicable action must explicitly respect privacy boundaries and encryption protocols. Imposing an obligation on underlying platform providers or API networks to inspect private payload data, break end-to-end encryption, or proactively monitor transmitted content creates significant compliance friction and directly conflicts with broader Australian Privacy Principles and international data protection standards.

3.14 **We submit that the Bill or, at least, the Explanatory Memorandum establish clear boundaries around what constitutes reasonably practicable technical compliance for infrastructure enablers if those are included in the scope of the DDOC at all.**

2. BUSINESS AND ENTERPRISE SERVICES

3.15 Some services that C/CSPs provide to enterprises may be considered social media services, relevant electronic services, or designated internet services within the meaning of the OSA and could, as such, potentially be considered in scope of a DDOC.

3.16 We have previously argued that any services provided by C/CSPs to enterprises (e.g. business-focused unified communications and cloud services, Communications Platform as a Service (CPaaS), APIs, transactional messaging infrastructure (e.g. MFA), business email platforms for resale to enterprise customers, software ecosystems built on developer APIs and independent software vendors) do not meet the risk threshold (and often also not the other thresholds of visibility/control, legal limitations) for inclusion in a DDOC.

3.17 In recent discussions with the Department, we were advised that the Bill was not intended to capture business-to-business and enterprise services. However, we believe that this is not clear from the current drafting of the Bill.

3.18 **Consequently, we submit that business and enterprise services provided by C/CSPs ought to be specified as exempt from the scope of the DDOC.**

4. APPS OR WEBSITES FOR THE MANAGEMENT OF C/CSP SERVICES

4.1 C/CSPs may provide websites or apps designed to allow customers to manage their services, including

prepaid services, which may be purchased by children. Such services are designated internet services within the meaning of the OSA.

4.2 These services also do not meet the risk threshold (and potentially also not the other thresholds of visibility/control, legal limitations) for inclusion in the DDOC.

4.3 **We submit that the use of such services for the purposes of facilitating telephony services ought to be specified as exempt from the scope of the DDOC as they pose an even lower risk than the telephony services that they are directly related to.**

5. RESALE OF SERVICES AND EQUIPMENT

5.1 C/CSPs may resell social media services, relevant electronic services, or designated internet services, for example gaming subscriptions, or entertainment services, such as television and music streaming services (where these services contain social features which enable users to post or share content like shared playlists, group watching features, or content recommendations).

5.2 C/CSPs may also resell equipment and, depending on definitional aspects, may be considered 'manufacturers' of equipment where they re-brand equipment but do not take part in actual manufacturing (in the ordinary use of the term) of the equipment.

5.3 Under these arrangements, C/CSPs have limited control over the provision of the service, which is managed by the relevant provider. Typically, the role of C/CSPs in these services is limited to facilitating access to and billing of those services. In the case of the resale or 'manufacturing' of equipment, C/CSPs have no control over the equipment. Instead, the control either rests with the actual manufacturer of the equipment or, most likely, with the provider of the operating system of the equipment.

5.4 **We submit that the resale of such services by C/CSPs ought to be specified as exempt from the scope of the DDOC. We also submit that the resale and 'manufacturing' of equipment in cases as described above ought to be excluded from the scope of the DDOC. Instead, any DOC ought to be placed, if at all, on the controllers of the operating system.**

3. FEEDBACK FEATURES

5.5 Section 25F(5) recognises 'feedback features' as a design feature of a service.

> (5) An online service has a ***feedback feature*** if the service can display information to an end-user about:
>
> (a) the extent to which other end-users have viewed or otherwise engaged with material posted by the end-user on the service; or
>
> (b) the extent to which other end-users have opted to receive notifications about the end-user's account or material posted by the end-user on the service.

5.6 Section 25(B)(1)(b)(ii), in turn, links design features to 'harms' which are defined very broadly and non-exhaustively in section 25(E).

5.7 The definition of feedback features would, as currently drafted, include feedback indicating whether a communication has been received and/or viewed/read. For example, it would include the grey/blue ticks that are displayed for WhatsApp messages to indicate the status of a communication. Similarly, it would include feedback that indicates whether a message or email has been read.

5.8 Feedback features could also be interpreted to encompass automated developer event callbacks, delivery status webhooks, and transmission logs used strictly for core system operations, such as confirming the delivery of critical security verification codes or transactional alerts.

5.9 Given the broad definition of harms in section 25(E), it is unclear whether such feedback features could be considered causing 'harms'.

5.10 While C/CSPs at present may not provide services that include such receipt/read feedback, we believe that the extension of the DDOC to such features is impractical and not aligned with its intended purpose and operation.

5.11 With the dynamic evolution of technology, including rich communications services which may, in the future, be provided as part of a carriage service, **we submit that the definition of feedback feature ought to be amended to exclude mere receipt, read, forward etc. feedback features that otherwise do not convey engagement with the communicated content. We also submit that automated developer event callbacks, delivery status webhooks, and transmission logs used strictly for core system operations are excluded from the definition.**

5.12 Similarly, the definition of 'recommender feature' would encompass benign advertisements or content suggestions displayed to a user based on previous preferences. For example, this could include the recommendation of a specific device (e.g. a specific modem, router, or mobile device) which can be (or may be recommended to be) purchased with a service plan that a user has selected.

5.13 Given the very broad definition of harms, it is unclear whether such types of recommender features would be considered falling with that definition.

5.14 **We submit that the definition of 'recommender feature' be more targeted by specifying the types of material that are recommended through the feature to remove the uncertainty associated with the assessment of whether a design feature may cause harm. Alternatively, or additionally, we recommend narrowing the definition of harm.**

6. RISK ASSESSMENTS

6.1 The Bill proposes risk assessments be conducted by all regulated entities on an at least an annual basis and prior to the introduction of changes that could pose additional risks. The Bill proposes numerous items that must be included in a risk assessment. The eSafety Commission can determine additional items of content to be included in the risk assessments.

6.2 In line with the Productivity Commission's recommendations to reduce red tape and regulatory burden, and building on our feedback on the role, capability, and compliance with existing regulation by C/CSPs, **we submit that C/CSPs ought to be exempted from the requirements to provide annual risk assessments. At the very least, if risks assessments are required, these ought to be very limited in nature and upon request by the eSafety Commissioner only**.

6.3 We understand from recent discussions with the Department that a 'minimalist approach' to risk assessments for C/CSP services may be contemplated. We would welcome this approach.

6.4 However, we note that the proposed section 26A(4) does not permit the eSafety Commissioner to limit the content or frequency prescribed for risk assessments in section 26A(2) but merely permits an extension of such content and increased frequencies for assessments.

6.5 **In the absence of a complete exemption from risk assessments for low-risk services, we submit that Section 26A(4) ought to be amended to permit a more limited approach to risk assessments for low risk services.**

7. COMPLAINT AND DISPUTE PROCESS

7.1 The Bill proposes requirements for the availability of, and compliance with, complaint and dispute processes for prescribed online services.

> **26F Complaint and dispute processes**
>
> (1) A person responsible for a prescribed online service must:
> (a) have complaint and dispute processes that are available equally to all Australians; and
> (b) comply with any requirements determined by the Commissioner in relation to those processes.
>
> (2) A ***prescribed online service*** is an online service in a class of online services determined by the Commissioner under subsection (3).
>
> (3) The Commissioner may, by legislative instrument, determine:
> (b) requirements for the purposes of paragraph (1)(b); and
> (a) classes of online services for the purposes of subsection (2).

7.2 C/CSPs already comply with extensive and prescriptive requirements under

a) the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018,* including in relation to membership with the Telecommunications Industry Ombudsman (TIO) scheme;

b) the existing Class 1 and 2 Online Safety Codes and Class 1 RES and DIS Standards; and

c) the Scam Prevention Framework (SPF) and its subordinate instruments, including in relation to membership with the Australian Financial Complaint Authority (AFCA) scheme.

7.3 As indicated, C/CSPs do not have visibility of or editorial control over content.

7.4 **We submit that C/CSPs ought not to be required to provide any additional assistance in relation to complaints arising from the DDOC beyond these existing requirements, and that the eSafety Commissioner ought not be permitted to prescribe additional requirements in relation to complaint and dispute resolution for C/CSP services.**

8. DIGITAL DUTY OF CARE GUIDELINES

8.1 Section 26E permits the eSafety Commissioner to make guidelines to assist regulated entities with their compliance with DDOC requirements.

8.2 **We submit that the timely provision of guidelines ought to be required (rather than a permitted action) and that in doing so the eSafety Commission ought to be required to consult for 30 days with the relevant sectors affected by the DDOC.**

9. ENFORCEMENT AND PENALTIES

9.1 Given the complex regulatory environment that the DDOC interacts with, it is important that the regulated entity clearly understand the interaction of enforcement and penalty regimes of the regulatory ecosystem the DDOC operates in.

9.2 **Therefore, we ask that Department and the eSafety Commissioner provide explicit clarity on how civil penalties, administrative notices, and enforcement powers under the DDOC will operate alongside existing statutory enforcement mechanisms. This includes articulating how DDOC enforcement interacts with regulatory powers under the *Telecommunications Act 1997*, the Scam Prevention Framework, and Australian Privacy Principles, ensuring that C/CSPs are not subjected to overlapping or conflicting regulatory enforcement actions.**

Ends

Australian
Telecommunications
Alliance

Level 25 / 100 Mount Street
North Sydney NSW 2060

T 02 9959 9111
E info@austelco.org.au
W austelco.org.au

ABN 56 078 026 507

