

30 October 2026

BSA SUBMISSION ON THE ONLINE SAFETY AMENDMENT (DIGITAL DUTY OF CARE) BILL 2026

Submitted Electronically to the Senate Environment and Communications Legislation Committee (the Committee)

The Business Software Alliance (**BSA**)¹ welcomes the opportunity to provide comments to the Committee on the Online Safety Amendment (Digital Duty of Care) Bill 2026 (**Bill**).²

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud services, collaboration systems, enterprise software and cybersecurity solutions, which many Australian companies and government agencies rely on.

BSA filed comments on the Exposure Draft of the Bill (**Exposure Draft**) with the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts on 22 September 2026.³ In that submission, and in our engagements at every stage of Australia's online safety framework since 2021,⁴ we have consistently advocated that services designed for business-to-business use should be excluded from obligations designed for consumer-facing services. Our below comments on the Bill and the proposed Digital Duty of Care (**Duty**) reflect these long-held positions.

Business-to-Business Services Should Be Excluded from the Digital Duty of Care

The Bill imposes the Digital Duty of Care (**Duty**) on every "person responsible for an online service", requiring such persons to take appropriate action to ensure "a safe online

¹ BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

² Online Safety Amendment (Digital Duty of Care) Bill 2026, October 2026, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r7553.

³ BSA Submission on the Exposure Draft of the Online Safety Amendment (Digital Duty of Care) Bill 2026, September 2026, <https://www.bsa.org/policy-filings/australia-bsa-comments-exposure-draft-online-safety-amendment-digital-duty-of-care-bill-2026>.

⁴ See:

- BSA Response to the Online Safety Bill 2020 Consultation, February 2021, <https://www.bsa.org/files/policy-filings/02122021ausonlinesafety.pdf>;
- BSA Comments to the Online Safety Bill 2021 Committee Inquiry, March 2021, <https://www.bsa.org/policy-filings/australia-bsa-submission-to-the-online-safety-bill-2021-committee-inquiry>;
- BSA Comments on the draft Online Safety (Basic Online Safety Expectations) Determination 2021, November 2021, <https://www.bsa.org/policy-filings/australia-bsa-comments-on-basic-online-safety-expectations>;
- BSA Comments on Australia's Draft Online Safety Industry Standards for Designated Internet Services and Relevant Electronic Services, January 2024, <https://www.bsa.org/policy-filings/australia-bsa-comments-on-draft-online-safety-industry-standards>.

environment”.⁵ “Online service” covers every category already regulated under the *Online Safety Act 2021 (Act)*, including Relevant Electronic Services (**RES**), Designated Internet Services (**DIS**) and Hosting Services.⁶ The Explanatory Memorandum confirms that “the Duty applies to all online services under the Act”.⁷

Although the Bill is clearly designed to improve safety for consumers, its scope is not limited to consumer-facing services and does not exclude business-to-business services. The only relief for providers of business-to-business services is section 25B(3), under which the Minister may, by legislative instrument, exempt an online service or a class of online services from one or more provisions of Part 2 if satisfied that the service or class “pose little risk to users of the service or services in Australia” after seeking the Commissioner’s advice.⁸

This raises three concerns.

First, the Act’s definitions are overly broad and reach well beyond consumer-facing services, ultimately capturing business-to-business services with a fundamentally different risk profile than consumer technologies.

As it stands, the Act’s categories of RES, DIS, and hosting services capture workplace collaboration tools, software-as-a-service applications of every kind, and the cloud infrastructure on which customers store material. **For business-to-business purposes, the relevant “online services” are used by the employees, contractors, and customers of the enterprise customer pursuant to that enterprise customer’s purposes and established policies and regulatory requirements.**

The Bill has broadened these definitions further – the new paragraph 25B(1)(h) captures any service “generate material using artificial intelligence, using an internet carriage service in the course of doing so” as an online service.⁹ This is broader than the Exposure Draft, which covered only services allowing users to generate material by AI and share it through another online service. Consequently, the Duty would now also apply to business-to-business services with AI features that generate outputs for an organisation’s internal use, even where those outputs are never shared or made available to anyone else.

In the recent Framework Paper on developing the Duty, it was acknowledged that obligations should be “proportionate to a service’s risk profile and their opportunity to address risks”.¹⁰

⁵ Bill, Schedule 2, Part 1, item 8 (new sections 25B(2) and 26(1)).

⁶ *Online Safety Act 2021*, sections 13A, 14 and 17. A **RES** includes a service that enables end-users to communicate with other end-users by email, instant messaging, SMS, MMS or chat, and a service that enables end-users to play online games with other end-users (section 13A). A **DIS** is a service that allows end-users to access material using an internet carriage service, or that delivers material by means of an internet carriage service, other than a social media service, relevant electronic service, on-demand program service or a service specified by the Minister (section 14). A person provides a **hosting service** if the person hosts stored material that has been provided on a social media service, relevant electronic service or designated internet service, whether or not that person also provides the service on which the material is provided (section 17).

⁷ Explanatory Memorandum, p. 52.

⁸ Bill, Schedule 2, Part 1, item 8 (new subsection 25B(3)). Before making the instrument, the Minister must seek and have regard to the Commissioner’s advice (new section 28B). BSA also notes that the same provision in the Exposure Draft also covered services “used minimally in Australia” – this was not retained in the Bill.

⁹ Explanatory Memorandum, p. 51. See also Bill, Schedule 2, Part 1, item 8 (new paragraph 25B(1)(h)).

¹⁰ Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, *A Digital Duty of Care for Australia: Developing a Duty of Care Framework for Online Services used by Australians*, May 2026,

However, the Bill would apply the same statutory duty and maximum penalties to a workplace collaboration tool as to a consumer social media platform, even though they have vastly different risk profiles. The Bill has also narrowed the room for proportionality. Section 26(1) of the Exposure Draft required a person responsible for an online service to ensure a safe online environment “so far as is reasonably practicable”, and section 25H defined that expression to include whether the cost of a measure was grossly disproportionate to the risk. Neither provision appears in the Bill.

Conduct on business-to-business systems is, moreover, already governed by workplace, contractual, and sector-specific laws and by the terms the organisation sets for its own staff and customers. The Duty would layer a second, general regime over arrangements that already allocate responsibility to the relevant organisations. The effect is to require risk assessments from services the Duty was never intended to cover.

Second, business-to-business service providers cannot discharge the Duty because they have neither a direct relationship with individual consumers nor access to their data.

Business-to-business service providers provide solutions to other organisations which enable their employees, contractors, and customers to use these technologies for various commercial and organisational purposes. As such, a business-to-business service provider usually has no direct relationship with individual customers of their business clients and would not know which individual client customers, if any, are children.

Furthermore, business-to-business service providers are subject to technical, legal, and contractual obligations that generally prohibit them from inspecting their enterprise customers’ data except in limited circumstances.¹¹ Access to customer content is deliberately limited by privacy and security controls built into the enterprise products and services, including customer-managed encryption, because enterprise customers, including government agencies and critical infrastructure operators, require it. A business-to-business service provider therefore could not moderate material it does not have the right to access. Nor should it be required to alter design features its enterprise customer configured. The entity in the best position to take such actions is the enterprise customer, which sets the terms of use, configures the service, and has a direct relationship with individual users.

This concern is further exacerbated by the definition of a “person responsible” in section 25B(2) of the Bill, which covers both “the person who provides the service” and “the person who exercises the greatest degree of day-to-day control over the service”. This assumes that an entity that provides a service always has full visibility of end-user data and control over how the service is used, which, as set out above, is not the case for a business-to-business service provider.

The practical consequence is clearest in the risk assessment aspect of the Duty. A business-to-business service provider with no meaningful visibility into how its enterprise customers have configured the service would nonetheless be required, under section 27, to conduct written risk assessments identifying reasonably foreseeable risks, the material or conduct giving rise to them,

<https://www.infrastructure.gov.au/sites/default/files/documents/digital-duty-of-care-for-australia-developing-duty-of-care-framework-for-online-services-used-by-australians-may2026.pdf>.

¹¹ See the submissions listed at footnotes 3 and 4. See also How Enterprise Software Empowers Businesses in a Data-Driven Economy, <https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf>.

the design features involved, and the persons who may be affected. In practice, the provider is required to assess risks that it cannot observe.

Third, the ministerial exemption power does not give business-to-business providers or their customers the certainty they need.

Section 25B(3) allows the Minister, by legislative instrument, to exempt an online service or class of online services from one or more provisions of Part 2 if satisfied that the service or class “pose little risk to users of the service or services in Australia”.¹²

BSA recognises that such a power has a proper role in a framework that must adapt to new services and harms. However, as this power can only be exercised when the Duty takes effect 12 months after Royal Assent, business-to-business service providers and their customers will not have a clear indication of whether the Duty applies to them or, if so, who is responsible for meeting it. The Bill also sets no criteria against which the Minister is to assess whether a service poses little risk, and no process by which a provider may seek an exemption.

Where it is already clear that a class of online service poses little risk to individual Australians, as is the case for business-to-business services, the exclusion should be stated in the Act rather than left to a later instrument.¹³ The low risk (to individuals) profile of business-to-business services is not a matter awaiting assessment. It follows from how these services are supplied and controlled, and it has already been recognised in the registered industry codes, which define “enterprise DIS”, exempt them from risk assessments, and deem them to be categorised in the lowest risk tier.¹⁴

Recommendations

In view of the above concerns, BSA recommends that the Bill be amended to:

- insert an express exclusion in section 25B for services provided to a business, government agency or other organisation for its internal use under contract. The definition of “enterprise DIS” in the registered industry codes provides a ready basis for the drafting;
- limit paragraph 25B(1)(h) to services that generate material using AI and make that material available to the public;
- add statutory criteria to section 25B(3) for any residual exemptions, and a process by which a provider may seek one, so that providers can assess in advance whether a service is likely to qualify; and

¹² Bill, Schedule 2, Part 1, item 8 (new section 25B(3)).

¹³ Other jurisdictions have drawn this distinction in the legislation itself. For example, under the European Union’s Digital Services Act, the obligations imposed on online platforms attach only to hosting services that disseminate information “to the public”, which means making it available to “a potentially unlimited number of third parties”. See Regulation (EU) 2022/2065, Article 3(i) and (k). Recital 14 confirms that, where access requires registration or admittance to a group of users, information is disseminated to the public only where users are admitted automatically and without a human decision as to who is granted access. A service supplied to a defined group of an organisation’s personnel and authorised contractors therefore falls outside those obligations. Similarly, the United Kingdom’s *Online Safety Act 2023* exempts internal business services that are available only to a closed group comprising a business’s officers, staff and authorised contractors (Schedule 1, paragraphs 7 and 8).

¹⁴ Designated Internet Services Online Safety Code (Class 1C and Class 2 Material), clauses 3(f) and 4.4(f), <https://www.esafety.gov.au/sites/default/files/2025-09/Schedule-6-Designated-Internet-Services-Online-Safety-Code-Class-1C-and-Class-2-Material.pdf>.

- limit “persons responsible” under subsection 25B(2) to those who exercise the greatest degree of day-to-day control of the service; and
- restore the “reasonably practicable” qualification to section 26, and provide that technical feasibility and the cost of a measure may be taken into account under section 26A.

If the Committee does not recommend a statutory exclusion, the Bill should, at a minimum, require the Minister to make an exemption under section 25B(3) that addresses business-to-business service providers.

Conclusion

We thank the Committee for the opportunity to provide these comments. BSA supports the Government’s objective of a safer online environment for Australians, and our recommendations are directed at ensuring the Duty reaches the services where the harms it addresses actually arise. Business-to-business service providers pose little risk to Australians online, contribute to their security and privacy, and are not in a position to discharge obligations designed for the platforms that do. We would welcome the opportunity to assist the Committee further as it considers the Bill.

Yours sincerely,

Tham Shen Hong
Director, Policy – APAC