

22 September 2026

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

Submitted Electronically to the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (the Department)

The Business Software Alliance (**BSA**)¹ welcomes the opportunity to respond to the Exposure Draft of 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 has engaged at every stage of Australia's online safety framework, including the *Online Safety Bill* and the *Basic Online Safety Expectations* in 2021, the industry codes as a member of the industry steering group, and the industry standards in 2024.³ In our engagements, 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 Duty on every "person responsible for an online service", requiring such persons to ensure "a safe online environment".⁴ "Online service" covers every category already

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 Exposure Draft, Online Safety Amendment (Digital Duty of Care) Bill 2026, September 2026, <https://www.infrastructure.gov.au/departments/media/publications/exposure-draft-online-safety-amendment-digital-duty-care-bill-2026>.

³ 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>.

⁴ Bill, Schedule 2, item 7 (new sections 25A(2) and 26(1)).

regulated under the *Online Safety Act 2021 (Act)*, including Relevant Electronic Services (**RES**), Designated Internet Services (**DIS**), and Hosting Services.⁵ The person responsible must also manage design features, conduct annual risk assessments under section 26A, and take effective measures.⁶

Although the Bill is clearly designed to improve safety for consumers, its scope is not limited to consumer-facing services and does not clearly exclude business-to-business services.

The only relief for providers of business-to-business technologies is section 25A(3), under which the Minister may exempt services that “pose little risk to users of the service in Australia” or “are used minimally in Australia”, after seeking the Commissioner’s advice.⁷

This raises three significant 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. But these services can be used for either consumer-facing or business-to-business purposes. 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.

In its recent Framework Paper on developing the Duty, the Department recognised that obligations should be “proportionate to a service’s risk profile and their opportunity to address risks”.⁸ However, the Bill would apply the same Duty (and penalties) to a workplace collaboration tool as to a consumer social media platform, even though they have vastly different risk profiles. 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.⁹ The Duty would layer a second, general regime over arrangements that already allocate responsibility to the relevant organisations.

⁵ *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).

⁶ Bill, Schedule 2, item 7 (new sections 26(3) and 26A).

⁷ Bill, Schedule 2, item 7 (new sections 25A(3) and 27B).

⁸ 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, <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>.

⁹ BSA Comments to the Online Safety Bill 2021 Committee Inquiry (2021), p. 2.

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. 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.¹⁰ 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.¹¹ The entity in the best position to take such actions is the enterprise customer, which sets the terms of use and has the direct relationship with individual users.

This concern is further exacerbated by the proposed definition of a "person responsible" in the Bill, which currently covers both "a person who provides the service" and "a person who is in a position to exercise day-to-day control of 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.

Third, the ministerial exemption power in section 25A(3) does not give business-to-business service providers or their customers the certainty they need.

Section 25A(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[s] little risk to users of the service in Australia" or is "used minimally 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 after the Duty takes effect, 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. 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. 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

¹⁰ See the submissions listed at footnote 3. See also How Enterprise Software Empowers Businesses in a Data-Driven Economy, <https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf>.

¹¹ Many business-to-business service providers offer configurable platforms that enterprise customers deploy for their own purposes and users. In the context of the proposed obligations e.g., conducting risk assessments under section 26A, a business-to-business service provider without meaningful visibility into how enterprise customers have configured the service is essentially required to assess risks that it cannot observe.

¹² Bill, Schedule 2, item 7 (new section 25A(3)).

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.¹³

Recommendations

In view of the above concerns, BSA recommends that the Bill: a) clearly set out that the Duty will *not* apply to an entity acting in its capacity as a provider of a business-to-business service; and b) limit "persons responsible" to those who are in a position to exercise day-to-day control of the service. If the Department does not adopt a statutory exclusion, the Bill should, at a minimum, require the Minister to make an exemption under section 25A(3) that addresses business-to-business service providers. In the meantime, the Department should extend the transition period to at least 24 months from Royal Assent, so that exemption can be made and businesses can adjust their compliance frameworks accordingly.

Conclusion

We thank the Department for the opportunity to provide our recommendations in response to the Bill. BSA supports the Government's objective of a safer online environment for Australians, and our recommendations are directed at ensuring the Duty is not extended to business-to-business service providers, which 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 welcome the Department's continued engagement with industry stakeholders, including BSA and our members, and we look forward to continued dialogue as the Bill progresses.

Yours sincerely,

Tham Shen Hong
Director, Policy – APAC

¹³ 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?v=1788739200044>