Cisco Systems, Inc. Comments
July 2023

Response to Department of Industry, Science and Resources Consultation: Safe and responsible AI in Australia

Executive Summary

Cisco Systems, Inc. (Cisco) hereby files comments in response to the Department of Industry, Science and Resources' (DISER) Consultation on "Safe and responsible AI in Australia", dated June 2023.

Potential of AI

Artificial Intelligence (AI) has immense potential to positively transform economies, businesses, and lives around the globe. For Australia, AI presents significant opportunities in driving economic growth and improving public goods and social outcomes. As an enabling capability, AI is already being integrated into Australians' homes and workplaces to realise practical use cases across various industries, resulting in greater productivity and substantial cost savings for businesses, coupled with improved experiences for consumers. As the technology develops and the public grows in confidence and demands towards AI use, we can expect AI to have an even greater impact on society.

Responsible AI use

To maximise benefits to society, responsible development and application of AI is key. Cisco firmly concurs with the Australian Government that AI use must be done responsibly to mitigate the potential risks as outlined in the discussion paper. Cisco recognises there needs to be clear principles and guidelines for responsible and inclusive AI use to mitigate such current and emerging risks. Thus, Cisco has articulated its Responsible AI Principles as governance tenets for developing, deploying or using AI capabilities in Cisco. To complement this, Cisco's Responsible AI Framework sets out how these principles are practically applied throughout Cisco's product and service lifecycles.

A risk-based regulatory approach that supports innovation

Cisco encourages DISER to consider taking a **pro-innovation risk-based approach** to regulating AI, adopting regulations that are differentiated and proportionate to the risk factors of use cases, and not regulations that are broad-brushed in nature and cover entire sectors or technologies. Regulations should be focused and applied to only "high-risk" use cases that warrant greater intervention to mitigate higher likelihoods of unfavourable outcomes. Where existing legal protections can be relied upon concerning privacy, data protection, security, discrimination, and human rights, new AI-specific regulation should be avoided to prevent duplication of regulations. Industry-led standards and guidelines should be prioritized over regulation, and where possible, harmonised and interoperable with internationally recognized standards.

Cisco's comments on draft risk-management approach

Cisco affirms DISER's proposed risk-management approach as indicated in Box 4 of the discussion paper, as well as the elements of the draft risk-based approach as outlined in Attachment C. They broadly align with the pro-innovation risk-based approach that Cisco recommends. Cisco offers some specific suggestions and observations in the submission that follows.

Cisco appreciates the opportunity to provide the above input to DISER's Consultation. Effective and efficient regulation of AI is important for Australia as it seeks to be a global AI leader. We would be happy to provide further information, input or advice regarding any discussion point.

Contact Information

For more information, please feel free to reach out to the following:

- Tim Fawcett, Director of Government Affairs, Cisco Australia (tifawcet@cisco.com)
- Seow Hiong Goh, Executive Director of Global Policy and Government Affairs (Asia Pacific), Cisco (shgoh@cisco.com)

Introduction

Cisco Systems, Inc. (Cisco) hereby files comments in response to the Department of Industry, Science and Resources' (DISER) Consultation on "Safe and responsible AI in Australia," dated June 2023.

Cisco is a global provider of Internet Protocol (IP)-based networking solutions with a strong presence in Australia. Cisco is committed towards improving Australia's society and economy through the power of connectivity and technology, including AI. Cisco's *Australian Country Impact Plan* has three pillars: human capital, healthy communities and innovation economy. Within these three pillars, Cisco makes investments to support Australia's national priorities which include health, education, jobs and economic growth, sustainability, rural and regional Australia, SMBs and national security.

As part of our *Country Impact Plan*, Cisco's *Country Digital Acceleration* program makes investments, including in AI specific projects. In 2021, Cisco partnered with New South Wales Transport to run AI and Internet of Things (IoT) trials to optimise public transport[1]. Currently, Cisco has established a Research Chair at La Trobe University supporting AI and IoT research at the university and establish a Cisco Innovation Central in Melbourne[2]. Cisco is also a founding industry member of the Cyber Security Cooperative Research Centre and supports many research programs including the AI-focused Augmenting Cyber Defence Capability project.

Given this Australian activity and the existing Machine Learning (ML) and AI in Cisco products and offers, Cisco welcomes the Australian Government's consultation on "Safe and Responsible AI in Australia" as a measured approach in mitigating potential risks from AI, whilst increasing public trust and literacy in AI's development and use. Overall, Cisco recommends a pro-innovation, risk-based approach towards regulation with risk-based and proportionate regulations for high-risk use cases.

Potential of AI

Artificial Intelligence (AI) has immense potential to positively transform economies, businesses, and lives around the globe at an accelerated pace. The global AI market is estimated to be worth USD 136.6 billion in 2022 and is projected to grow at a staggering compound annual growth rate of 37.3% from 2023 to 2030[3]. This growth is testament to the advantages of using AI, which are manifold. These range from increased productivity, improved accuracy and carrying out dangerous or menial jobs, to big data analysis, personalised citizen/customer experiences and more efficient back-of-house functions.

AI has also been the basis for a range of new scientific breakthroughs, with the likes of machine learning (ML), deep learning, neural networks, expert systems, natural language processing (NLP), generative systems, and computer vision that are continually being rolled

[1] https://www.zdnet.com/article/nsw-transport-and-cisco-to-run-ai-and-iot-trials-to-ease-congestion-on-public-transport

[2] https://www.cisco.com/c/m/en_au/niin/researchchairs.html#~research-chairs

[3] https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market

out and refined. These technologies will allow for faster and more advanced ways of doing business and providing public services and are expected to evolve in complexity and bring about fundamental changes to the modern world.

For Australia, AI presents significant opportunities to improve the nation's economic and social outcomes, and Cisco notes that AI has been highlighted as a critical technology in Australia's national interest. As an enabling capability, AI is already being integrated into Australians' homes and workplaces to realise practical use cases across various industries. These range from optimised logistics and operations[4] to personalised and enhanced healthcare[5] and legal[6] services, all powered by data-driven decision-making. Such innovation results in greater productivity and substantial cost savings for businesses, coupled with improved experiences for consumers. Australian companies see the value AI brings and are willing to invest in the technology, with spending on AI expected to double to USD 3.6 billion by 2025[7]. Indeed, as the technology develops and the public grows in confidence and demands towards AI use, we can expect AI to continue being integrated into how people live, work and play and learn.

Responsible AI Use

Cisco firmly concurs with the Australian Government that AI use must be done responsibly, to mitigate potential risks.

Cisco's Approach to AI

Cisco increasingly uses AI and ML across its product and service portfolio to enhance functionalities and improve user experience. This allows Cisco to, for example, provide intelligent and exciting new user interfaces through our collaboration tools[8], understand and manage network traffic more effectively and predictively[9], or identify and block cyber threats[10]. In workforce development, Cisco also leverages AI- and ML-based tools to hire and evaluate potential job candidates more effectively.

Cisco believes that privacy, security, and inclusion must be central in design methodology. The applications of AI in Cisco's current technologies are responsibly developed, with informed consent. Cisco minimises personal or sensitive data collected from customers and

[4] https://www.coragroup.com.au/the-future-is-here-ai-in-australian-logistics-and-what-it-means-for-you
[5] https://aahms.org/news/roundtable-report-ai-in-health
[6] https://blog.ai-laws.org/ai-in-law-firms-down-under-australian-law-and-the-rise-of-legal-tech
[7] https://www.idc.com/getdoc.jsp?containerId=prAP49145022
[8] Cisco has developed a suite of tools for collaboration and online meetings, events and webinars. These leverage AI and ML to identify participants, blur backgrounds and create meeting layouts. To facilitate clear communication, the tools also utilise speech detection and natural language processing to power a virtual assistant, record meeting transcripts, translate, reduce background noise, and optimize voice levels. https://www.webex.com
[9] Cisco also offers tools which use AI to help companies' IT administrations optimize networks, troubleshoot connectivity or configuration issues, predict traffic flows, and automatically optimize or remediate issues. https://blogs.cisco.com/networking/better-together-cisco-dna-center-and-thousandeyes
[10] AI and ML are also utilised in the area of cybersecurity, to detect, classify, and respond to known and novel malware, network anomalies and other threats.
https://www.cisco.com/site/sg/en/products/security/index.html

end users to what is strictly required to offer services. Cisco also seeks alternative product designs that avoid data collection where possible. Cisco is deliberate in decision-making about whether the use of technologies such as AI is appropriate to meet customer needs.

Even so, we recognize that by applying this technology, Cisco has a responsibility to mitigate potential harm. As outlined in the discussion paper, there are potential risks in utilising AI technology. These include the ability to generate and propagate misinformation, biases, and deep fakes, which have disproportionate impacts on vulnerable segments of society. These risks can be difficult to fully anticipate, given the rapid pace with which AI is developing.

Cisco's Responsible AI Framework

Hence, Cisco recognises there needs to be clear principles and guidelines for responsible and inclusive AI use to mitigate the current and emerging risks. These will serve as guardrails to counter inaccuracy, bias, privacy and security threats. To this end, Cisco has articulated its Responsible AI Principles[11] as governance tenets for developing, deploying and using AI capabilities in Cisco. There are six AI principles which Cisco abides by: Transparency, Fairness, Accountability, Privacy, Security, and Reliability. Each of these principles is a critical aspect to fair and responsible use of AI.

To complement this, Cisco's Responsible AI Framework[12] sets out how these principles are practically applied throughout Cisco's products and service lifecycles. Under such a framework, Cisco assesses AI functions for models and data directly involved in decisions that could have adverse legal or human rights impact. Controls are then applied to reduce risk of AI harm by targeting areas like unintended bias mitigation, model monitoring, fairness and transparency. Cisco believes that by scrutinizing biases in AI/ML models, there is an opportunity to address more explicitly some of the covert biases present even in traditional systems. We leverage security, data breach, and privacy incident response systems to manage and report AI incidents involving bias and discrimination. Cisco also supports AI incident reporting and rely on a governance committee to oversee responsible AI.

The key elements of the framework are set out below:

[11] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-responsible-artificial-intelligence-principles.pdf
[12] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-responsible-artificial-intelligence-framework.pdf

The Responsible AI Framework

Guidance and Oversight 	• Establishes a Responsible AI Committee of senior executives across Cisco business units, sales, privacy, security, human rights, legal, government affairs, human resources, and other functions. • Advises Cisco on responsible AI practices and oversees Responsible AI Framework adoption. • Reviews sensitive or high-risk uses of AI proposed by our business units and incident reports of bias or discrimination.
Controls 	• Embeds security, privacy, and human rights processes into AI design as part of the existing Cisco Secure Development Lifecycle. • Assesses AI functions for models and data directly involved in decisions that could have adverse legal or human rights impact. • Applies controls to reduce risk of AI harm by focusing on areas like unintended bias mitigation, model monitoring, fairness, and transparency.
Incident Management 	• Leverages security, data breach, and privacy incident response system to manage reported AI incidents involving bias and discrimination. • Assigns and reports incidents to the Responsible AI Incident Response Team to analyze and engage relevant team for resolution. • Tracks and reports AI incidents to governance board and reports findings and remediation steps to the original submitter or a broader group of stakeholders, customers, employees, and partners.
Industry Leadership 	• Embeds Responsible AI as a focus area for incubation of new technology across Cisco. • Engages with industry innovation providers focused on delivering Responsible AI. • Participates proactively in industry forums to advance Responsible AI, including the Centre for Information Policy Leadership, Equal AI, and the Business Roundtable on Human Rights and AI.
External Engagement 	• Works with governments to understand global perspectives on AI's benefits and risks. • Monitors, tracks, and influences AI-related legislation, emerging policy, and regulations. • Partners with and sponsors cutting-edge research institutions, exploring the intersection of ethics and AI from technical, organizational, social, and design perspectives.

A Pro-Innovation Risk-Based Regulatory Approach

To keep Australia competitive on an international level as a technology hub, Cisco encourages DISER to consider taking a **pro-innovation risk-based approach** to regulating AI. As part of such an approach, regulations should be differentiated and proportionate to the risk factors of use cases. This is opposed to having regulations that are broad brushed in nature and cover entire sectors or technologies. Cisco is of the view that the latter would be overly restrictive to both large and small companies who engage in AI use at low to moderate risk levels. Further, such blanket requirements would hinder overall industry innovation and agility. In taking a pro-innovation risk-based approach, Australia would continue to offer organizations room to innovate and develop technologies that offer net benefits to society.

Cisco proposes that regulations should be narrowly focused on specific "high-risk" use cases – with legal and human right ramifications – that warrant greater intervention to mitigate

higher likelihoods of unfavourable outcomes. Examples of such high risk uses cases would be the automated operation of critical infrastructure and public deployment of facial recognition and biometric identification. At the same time Cisco emphasizes the differences between high-risk (e.g., surreptitious/surveillance) use cases and consent-based, enterprise use of biometric identification. Requirements imposing mandates for transparency, documentation, consent, explicability, and human oversight can thus be applied to such uses of AI where the risk and impact is high.

Cisco recommends that where existing legal protections can be relied upon concerning privacy, data protection, security, discrimination, and human rights, new AI-specific regulation should be avoided to prevent duplication of regulations and an easier regulatory landscape for enterprises to navigate and comply with. In taking a pro-innovation risk-based approach, Australia would continue to offer businesses room to innovate and develop technologies which offer net benefits to society.

Cisco recommends that industry-led standards and guidelines should be prioritized over regulation. Given the dynamic pace of AI development and the concurrent growing awareness and demand for AI, nascent technologies require time to develop potential use cases that can benefit society. Industry-led standards are thus more suited as they offer much needed flexibility to adapt to evolving technology. Where possible, the approach should be harmonised and interoperable with internationally recognized standards, to allow Australian and Australia-based enterprises to transact across borders and maintain international competitiveness more seamlessly. This would also augment Australia's global standing as place of choice for AI investment and business. As a leader in responsible AI, Cisco would also encourage DISER to take a proactive stance to lead global conversations to arrive at aligned internationally recognized standards and approaches to regulating AI.

Cisco's Views on Australia's Proposed Approach (Box 4 and Attachment C)

Building on the principles articulated above that Cisco is taking towards AI, below are specific comments on Australia's proposed approach as articulated in the discussion paper for consideration.

Box 4: Possible draft risk management approach

> Cisco affirms DISER's proposed risk management approach as indicated in Box 4 of the discussion paper. In Cisco's view, this approach broadly aligns with the pro-innovation risk-based approach earlier recommended. Cisco agrees with the considerations listed out in adopting such an approach, specifically how it caters for context-specific risks, reduces onerous obligations for lower risk AI use cases, and allows AI to continue to be used in high-risk settings subject to higher constraints and checks.
>
> Specifically, for the use cases identified as low risk, we note that DISER had included mandatory user training. Cisco would like to caution against placing overly prescriptive obligations on enterprises and would suggest that such training not be mandated. Many low risk use cases are intended for the convenience and ease of

use by the user. As such, requiring explicit training would discourage its innovative use.

For the medium risk use cases, in the left most column of the table, we suggest removing the word "high" from the phrase "high impacts that are ongoing and difficult to reverse." The inclusion of the word "high" to describe medium risk use cases might be perceived as contradicting and hinder consistent understanding of the rubric.

Attachment C: Possible elements of a draft risk-based approach

Cisco appreciates DISER's acknowledgment that there needs to be a coordinated response from the Government and industry to manage the inherent opportunities and risks arising from AI. Below are some specific observations of the elements of the draft risk-based approach.

Impact assessment: Where such assessment needs to be done, Cisco requests DISER to provide guidance on the specific areas needed to assess an impact. Cisco believes that impact assessments would be critical as a targeted approach to high-risk use cases and to address potential adverse legal or human rights impact. This would facilitate risk mitigation and model monitoring and build-in fairness and transparency to the development and usage of AI.

Human-in-the-loop: As noted in the discussion paper, it is important to recognize that "human-in-the-loop" may not be required for all instances of AI use, particularly in low-risk situations. If "human-in-the-loop" measures were required for all forms of AI use, it would hamper innovation significantly.

Monitoring and documentation: Cisco agrees that this measure should be commensurate with the risk level of AI usage. Cisco would like to highlight that monitoring can be resource-intensive, as it involves internal coordination and input of the organization's senior executives as well as other cross functions deploying AI, and as such, should be explicitly planned for. Even so, monitoring is a useful tool to ensure that there is appropriate use of AI and address incidents which may arise out of high-risk or sensitive AI use cases.

Further to those proposed in the paper, an additional element to consider is incident management. Organizations should be expected to have clear channels for external parties contesting or seeking redress for AI decisions. Organizations should be made explicitly responsible in ensuring they have the right tools and skilled people for such incident management.

In the following section, Cisco offers our responses to specific questions raised in the discussion paper for DISER's consideration. We extend our gratitude to DISER for the opportunity to comment and look forward to partnering with the Government as conversation around AI progresses.

Contact Information

For more information, please feel free to reach out to the following:

- Tim Fawcett, Director of Government Affairs, Cisco Australia (tifawcet@cisco.com)
- Seow Hiong Goh, Executive Director of Global Policy and Government Affairs (Asia Pacific), Cisco (shgoh@cisco.com)

Responses to Questions Raised in the Discussion Paper (Chapter 5)

Definitions

1. Do you agree with the definitions in this discussion paper? If not, what definitions do you prefer and why?

- Cisco acknowledges that there are various ways of defining AI. We have referenced the definitions stated by the discussion paper for the purposes of this response submission.

Potential gaps in approaches

2. What potential risks from AI are not covered by Australia's existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks? 3. Are there any further non-regulatory initiatives the Australian Government could implement to support responsible AI practices in Australia? Please describe these and their benefits or impacts. 4. Do you have suggestions on coordination of AI governance across government? Please outline the goals that any coordination mechanisms could achieve and how they could influence the development and uptake of AI in Australia.

- We refer to the discussion above about adopting a **pro-innovation risk-based approach** to supporting the development of AI in Australia, allowing flexibility to ensure that enterprises are able to innovate, while still providing guidance to the industry through clear principles and practical advice. Australia's approach should promote a pro-innovation outlook and not a rigid regulatory approach.
- There is a need to provide for incident management and handling of instances of contesting or redress for AI decisions, in line with transparency expectations.
- Considerations of "fairness" should also emphasize inclusion as a key component so that as many people can benefit from the potential of AI as possible.
- In relation to non-regulatory initiatives, the government may wish to consider citizen education in areas such as the limitations of generative AI and large language models. This would help address mitigate concerns relating to misinformation and disinformation being extended to AI.

Responses suitable for Australia

5. Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?

- The United Kingdom has articulated a principles-based, risk-focused approach in its recent consultation by the Department for Science, Innovation and Technology[13] that is a good model. The details of implementation however may remain a

[13] https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach

challenge with how multiple regulators can effectively govern this cross-sector issue and the alignment with approaches taken in other jurisdictions.

Target areas

6. Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?
7. How can the Australian Government further support responsible AI practices in its own agencies?
8. In what circumstances are generic solutions to the risks of AI most valuable? And in what circumstances are technology-specific solutions better? Please provide some examples.
9. Given the importance of transparency across the AI lifecycle, please share your thoughts on:
    a. where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?
    b. mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.
10. Do you have suggestions for:
    a. Whether any high-risk AI applications or technologies should be banned completely?
    b. Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?
11. What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

- There is a need to consider and coordinate possible different approaches even as they are being taken by different Australian agencies covering their own sectors. There should be efforts to ensure consistency in execution and avoid regulatory overlap.
- On whether different approaches should apply to public and private sector use of AI technologies, we believe that taking a risk-based approach would be preferable rather than applying rules along sectoral lines.
- The public sector ought to be held to the same level of accountability and principles as proposed for the private sector when it comes to AI and Automated Decision Making (ADM), to retain public trust and deliver effective services[14]. It is the application and use of AI and ADM that requires responsible practice – not any specific entity.
- There are low, medium and high-risk applications of AI both in public and private sectors, and the approach should align with the appropriate risk level. E.g., a public deployment of facial recognition and biometric identification should be subject to the same considerations regardless of whether the deployment of the identification system for the generic public is by a public or private sector entity. In addition, to promote innovation, Australia may wish to consider excluding activities of research, testing and development from the scope prior to such AI systems being put in the market.

[14] https://robodebt.royalcommission.gov.au/

- There is a role that the Government can lead by example. We would encourage the Government to spearhead industry conversations, encourage private-public partnership models and lead-by-example in keeping to AI principles.
- The government is also the owner of extensive data sets that may be made available for AI systems. This may provide the opportunity for further digital innovation in government and delivery of services however, it is critical that government is held to same expectations as private organisations - if not higher as an exemplar. As such, it may be necessary to ensure that any government regulatory carve-outs or exemptions due to other applicable guidance do not go so far as to remove the need for such public accountability and appropriate oversight.
- On the importance of transparency across the AI lifecycle:
    - Cisco agrees that requiring organisations to make it clear when they are using AI would improve transparency.
    - In Cisco's own Principles for Responsible Artificial Intelligence published in 2022, we outlined transparency as one of six principles to guide how Cisco will develop, deploy and use AI capabilities. As such, we inform our customers when AI is being used to make decisions that affect them in material and consequential ways.
    - Regulators should avoid one size fits all information requirements and allow organisations deploying AI a degree of flexibility so that information provided is relevant, proportionate and is tailored to the use case, potential consequences and user.
    - Transparency requirements should be linked to contestability and redress principles covered. Cisco sees it as important that organisations deploying AI also have relevant governance and oversight as well as external engagement structures in place. By keeping communications channels open, Cisco intends to build, maintain, and grow the trust that our customers, users, employees and other stakeholders place in our AI offerings.
    - Cisco agrees that impacted third parties and actors in the AI lifecycle should be able to contest an AI decision or outcome that is harmful or creates material risk or harm.
    - A major part of getting this approach right is encouraging organisations deploying AI to have effective transparency and redress systems in place that are proportionate, risk based and straight-forward for users to engage with. As part of this transparency, organisations should take clear accountability for any decisions taken by their AI systems and offer redress should these decisions be incorrect or deficient.
- On Government initiatives or action to increase public trust in AI deployment, we believe there is a useful role Government can play in carrying out public education campaigns and integrate AI into their public services where appropriate.

Implications and infrastructure

12. How would banning high-risk activities (like social scoring or facial recognition technology in certain circumstances) impact Australia's tech sector and our trade and exports with other countries?
13. What changes (if any) to Australian conformity infrastructure might be required to support assurance processes to mitigate against potential AI risks?

- It is important to be clear on what constitutes a high-risk use case and to delink the technology underlying the application of the use case.
- There are cases where facial recognition technology is used responsibly in low-risk contexts in video collaboration tools such as Webex to perform functions such as virtual background and speaker identification in a meeting. However, Cisco agrees that there are higher risks context in instances of leveraging facial recognition and biometric identification in public settings.
- Broad stroke banning of activities might hinder tech sector and Australia's global standing as a leader in AI. Regulatory intervention should be applied only in specific uses where the risks clearly outweigh the positive outcomes in technology innovation.

Risk-based approaches

14. Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?
15. What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?
16. Is a risk-based approach better suited to some sectors, AI applications or organisations than others based on organisation size, AI maturity and resources?
17. What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?
18. How can an AI risk-based approach be incorporated into existing assessment frameworks (like privacy) or risk management processes to streamline and reduce potential duplication?
19. How might a risk-based approach apply to general purpose AI systems, such as large language models (LLMs) or multimodal foundation models (MFMs)?
20. Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to:
    a. public or private organisations or both?
    b. developers or deployers or both?

- We encourage an approach that ensures implementation in a way that is use-case focused, risk-based and proportionate, rather than focusing on entire sectors or technologies.
- Regulators should focus on high-risk use cases and not on the technology and should engage closely with industry/businesses when making regulatory changes.
- As the technology is nascent, policy makers should avoid finalising regulations and requirements while the use cases are still being worked out.
- Such an approach accords proportionate risk-management requirements and regulations on tiered use cases, thus balancing risk control and innovation.
- Cisco's comments regarding Attachment C have been provided in the earlier part of this submission.

- As noted earlier, new AI-specific regulation concerning privacy, data protection, security, discrimination, and human rights should be avoided where existing legal protections can be relied upon.
- Cisco encourages taking a responsible, deliberate approach to the use of publicly available “chat bots” powered by “large language models.” Cisco’s corporate policy for employees is to only use enterprise-licensed tools.
- As with any technology, there are shared responsibilities. At Cisco, we recognize that in applying AI technology, we have a responsibility to mitigate potential harm. That is why we have developed a robust Responsible AI Framework based on six principles of Transparency, Fairness, Accountability, Privacy, Security, and Reliability. This governs how we develop and use AI.
- Australia may also wish to consider guidance on responsible AI to be applicable beyond just developers and deployers, but potentially also for users of AI (i.e., where an organizer neither develops nor deploys AI, but knowingly use such systems). Depending on the use case, the relevant risks should also be considered.

Cisco appreciates the opportunity to provide the above input to DISER’s Consultation. The issue on hand is important for Australia as it carves out its standing as a global AI leader. We would be happy to provide further information with regard to any discussion point.