Indo-Pacific Economy Framework Consultation:
Microsoft submission, October 2022

Microsoft appreciates the opportunity to share our views on the Indo-Pacific Economic Framework (IPEF) as the Department of Foreign Affairs and Trade shapes Australia's positions in upcoming negotiations. We applaud the new initiative's focus on deepening economic relations in the Indo-Pacific and addressing global economic challenges, including with respect to fair and resilient trade; digital and emerging technologies; supply chain resilience; infrastructure, clean energy, and decarbonisation; and tax and anti-corruption.

We believe that trade policy can create a more prosperous, equitable, and secure future for everyone. Creating a robust digital economic framework in the IPEF can support broader goals such as economic inclusion, competitiveness in critical and emerging technologies, secure and resilient infrastructure and technology supply chains, responsible use of technology, and sustainability.

In our comments, we have not offered comprehensive views on negotiating objectives, but rather highlighted items of particular importance or where we believe we have unique insights.

1. Growing the Digital Economy: Advancing Digital Trade Rules and Promoting Digital Inclusion

In the IPEF's fair and resilient trade pillar, the Framework can help grow the digital economy across the Indo-Pacific by **securing acceptance of existing high-standard disciplines, further refining those disciplines and filling gaps, and engaging cooperatively to advance worker-centric priorities.**

IPEF parties including Australia have shown leadership in advancing digital economy-related cooperation in recent years. Several agreements, including the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) and bilateral digital agreements, provide a solid foundation for IPEF. These include, for example, important provisions related to cross-border data flows, risk-based approaches to cybersecurity, and protection of intellectual property and source code. We encourage IPEF parties to see these as a foundation, which the IPEF parties can update and build upon.

Technical barriers to digital trade.

A key area of uncertainty for businesses across the IPEF region engaging in digital trade lies in the area of technical barriers to trade. Existing trade rules largely do not require fairness and non-discrimination in standards-setting for digitally-enabled services as they do for goods trade: the World Trade Organization (WTO) Technical Barriers to Trade (TBT) Agreement requires WTO Member governments to use open, transparent and non-discriminatory procedures to develop regulations, standards, and conformity assessment systems, and to ensure national treatment for products imported from other Member country. Equivalent obligations do not exist with respect to digitally-enabled services trade.[1]

Companies across the IPEF region face a significant – and increasing – number of barriers to digital trade in the form of market-specific technical standards, testing and certification requirements, and security regulations. These market-specific requirements typically lack the transparency and due process associated with open, international standards development processes and have been used as a tool to protect local cloud service operators. In particular we see a risk that requirements imposed ostensibly to protect cybersecurity in practice have excluded companies from providing services that support digital trade, including cloud services. This risks cutting businesses across the IPEF region off from a foundational component of the region's digital infrastructure that is essential for digital transformation.

The more straightforward way to address this issue would be for the **IPEF digital trade pillar to require that a party's standards governing digitally-enabled services trade be adopted in a manner consistent with the principle of national treatment and the WTO TBT Committee's Decision on International Standards** (setting forth governing principles on transparency; openness; impartiality and consensus; effectiveness and relevance; coherence; and the development dimension).

Alignment of digital standards.

In addition to ensuring non-discriminatory treatment in standard setting, **we encourage using IPEF as a mechanism for securing greater alignment in digital standards, particularly in the cybersecurity space.** Microsoft daily receives more than 24 trillion threat signals from its global network and is investing $20 billion over 5 years into improved cybersecurity outcomes, helping to detect and prevent cyber threats for the customers of our cloud services.[2] Market-specific requirements ostensibly imposed to increase cybersecurity can, in our experience, risk worsening the overall security environment, by limiting the potential for businesses across the IPEF region from accessing these cutting-edge cybersecurity services.

[1] Though the General Agreement on Trade in Services (GATS) places certain obligations on WTO Members, a Member is only obligated to guarantee market access and national treatment for service sectors and modes of supply it includes in its Schedule of Specific Commitments. Moreover, existing service sectors do not clearly capture many digitally-enabled services.

[2] Microsoft Digital Defense Report at 3, Oct. 2021, *available at* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi; Rick Wagner, *Microsoft Expands on Cybersecurity Commitments for U.S. Government Agencies*, Microsoft in Business (blog), Sept. 23, 2021, *available at* https://cloudblogs.microsoft.com/industry-blog/microsoft-in-business/government/2021/09/23/microsoft-expands-on-cybersecurity-commitments-for-u-s-government-agencies/.

More broadly, alignment of digital standards across the Indo-Pacific – through use of globally recognised standards and best practices – would enable digital trade opportunities businesses across the IPEF region and reduce the substantial cost of compliance with local standards. This is true across a broad spectrum of areas ranging, for example, from the responsible use of artificial intelligence to a harmonised approach to technology accessibility standards for people with disabilities.

While complete alignment likely is too ambitious a goal, particularly where evolving and cutting-edge technologies are concerned, **IPEF should adopt modes of cooperation and information sharing regarding standards development and adoption, as well as the cross-border recognition of conformity assessment results.** Towards this end, IPEF economies could look to work completed in the Asia Pacific Economic Cooperation (APEC), particularly the Subcommittee on Standards and Conformity Assessment (SCSC).

Skilling and inclusion.

IPEF presents an important opportunity to **promote digital inclusion, equitable access to technology, and cyber-skilling and workforce development for the digital economy**. The Digital Economy Partnership Agreement (DEPA), reached in 2020 by Singapore, Chile, and New Zealand, contains a useful starting point for cooperation on these issues, and action by the private sector will also be essential to achieving substantial gains. In light of the estimated 3.5 million cybersecurity jobs that will be open globally by 2025, Microsoft has launched a campaign to skill and recruit hundreds of thousands of cybersecurity workers across 24 countries, including multiple countries in the Indo-Pacific.[3] Recognising the lack of diversity in the cybersecurity workforce, particularly with respect to gender, a specific goal of our program is to ensure traditionally excluded populations, including women, have opportunities to enter the cybersecurity workforce.

Microsoft is pleased to participate in the IPEF Upskilling Initiative launched on 8 September 2022. We have committed to skilling at least 1.8 million women and girls for tech and tech-enabled roles by 2025 across IPEF economies. Further focused public-private collaborations through the IPEF could identify additional skilling initiatives to pursue within participating countries.

2. Creating Resilient, Secure, and Trustworthy Technology Supply Chains

We welcome that one of the objectives of **IPEF is to strengthen secure, trustworthy technology supply chains,** including the ready availability of critical and emerging technologies from trustworthy sources.

Overall, we see the supply chain challenge as three-fold in nature, requiring both short-term and long-term action:

[3] Brad Smith, *America Faces A Cybersecurity Skills Crisis: Microsoft Launches a National Campaign to Help Community Colleges Expand the Cybersecurity Workforce*, Official Microsoft Blog, Oct. 28, 2021, *available at* https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce/; Kate Behncken, *Closing the Cybersecurity Skills Gap – Microsoft Expands Efforts to 23 Countries*, Official Microsoft Blog, Mar. 23, 2022, *available at* https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/.

• **Security & Integrity**: Ensuring components and systems protect against intentional malware, trojans, and defects. Security in critical infrastructure such as financial systems, healthcare systems, and national security systems is rooted in authentication at the layer of underlying hardware. *For example: Inscribing attestation at the wafer level.*

• **Continuity**: Ensuring that bottlenecks in the supply chain have limited exposure to disruptions caused by geopolitical, natural disaster, or other location-specific risks. *For example: Dependency on certain manufacturing hubs for raw materials or assembly.*

• **Visibility**: Assign/update risk factors like manufacturing output, shipping slowdowns, or other unexpected events that can cause economic harm and then running what/if scenarios. *For example: Determining impact from Suez Canal blockage.*

A natural byproduct of deepening economic relations through the IPEF should be a diversification of supply chains for IPEF parties, which will help improve continuity. We encourage IPEF parties to avoid overly restrictive and prescriptive policies that could prove counterproductive, which risks making supply chains less secure in the long run. **We believe that coordinated trade policies should encourage best practices and technology-enabled supply chain risk mitigation measures**.[4] Employed appropriately, a multilateral supply chain security policy that incentivises such measures – rather than one that imposes undue and unpredictable regulatory burdens – will better protect supply chain security and resilience.

In the information and communications technology sector, digitally-enabled solutions can be implemented in software, hardware, and data:

- **Software security practices and technologies can address risks by providing greater supply chain transparency and protecting software from being exploited by bad actors or for malignant purposes.** Relevant practices and capabilities include secure software development, build environment integrity, and providing software bill of materials (SBOM) information. Features include the ability to deploy trusted software updates, including for the firmware of compromised devices, and automating security policies to, for example, seek out and prevent placement of user or administrator credentials in software code and detect the usage of software containing known vulnerabilities.

[4] Sarah O'Hare O'Neal, *Microsoft Proposes Incentivizing Digital Solutions to Mitigate Supply Chain Risk*, Microsoft on the Issues (blog), Mar. 23, 2021, *available at* https://blogs.microsoft.com/on-the-issues/2021/03/23/incentivizing-digital-solutions-mitigate-supply-chain-risk/; Microsoft Comments on the Commerce Department's Securing the Information and Communications Technology and Services ("ICTS") Supply Chain Interim Final Rule, Mar. 22, 2021, *available at* https://www.regulations.gov/comment/DOC-2019-0005-0091; Microsoft Comments on Risks in the Information and Communications Technology Supply Chain, Nov. 4, 2021, *available at* https://www.regulations.gov/comment/BIS-2021-0021-0024; Microsoft Corporation Response to *Request for Public Comment: Risks in the Supply Chain*, Nov. 8, 2021, *available at* https://www.regulations.gov/comment/BIS-2021-0036-0091.

- **Security technologies built into hardware can further protect against supply chain risks.** Such solutions include hardware roots-of-trust to verify, protect or restore system, data or code integrity; secure co-processors for more robust identity verification; and, in appropriate cases, origin and identity attestation for components in a hardware system. Also, archiving trusted copies of hardware, firmware and the software necessary to operate that hardware – along with updated versions that might resolve security issues – would ensure that hardware and software can be retrieved and flashed with "known good" firmware in the event of an emergency that prevents access to firmware updates from the original supplier.

- **Data security technologies can protect exposure of sensitive data through the supply chain.** Features include digital rights management, information flow controls, data tagging, and, where appropriate, the use of secure virtual or data lockbox environments.

The IPEF parties can accelerate the development and deployment of these practices, capabilities, and features by **providing incentives for companies to adopt them and strengthening consistency across any emerging requirements that might impact their deployment**. Broader adoption of and consistent requirements for solutions designed to mitigate supply chain risks would strengthen security as well as expand the market for solutions, further accelerating their development and contribution to supply chain security.

3. Creating Resilient, Secure, and Trustworthy Critical Infrastructure

We welcome that the IPEF pillar on infrastructure, clean energy, and decarbonization aims to, among other things, help "close the region's infrastructure gap."[5] **We welcome the focus on 5G communications capabilities, and encourage IPEF parties to expand their efforts to include hyperscale public cloud services, additional telecommunications capabilities, and submarine cables.** We understand that similar work may be underway in the Quad Critical and Emerging Technology Working Group, among the United States, Australia, India, and Japan, and thus the IPEF may provide a platform to amplify and formalise initiatives the that key IPEF parties are already pursuing in the Indo-Pacific.

Cloud Services.

Cloud services are an essential contributor to the security and resilience of critical sectors of the economy as they modernise. **Aligning cloud-related standards among IPEF parties would deliver major benefits, especially through joint efforts to develop consistent and interoperable requirements on critical digital infrastructure.** This would result in increased security of cloud services and infrastructure – and the critical sectors that rely on them – across the IPEF parties, as well as setting a high bar that others would likely follow.

[5] White House, *Indo-Pacific Strategy of the United States*, Feb. 2022, at 11-12, *available at* https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.

While there is some alignment between certain potential IPEF countries in cloud services and infrastructure security requirements (e.g., FedRAMP in the United States; ISMAP in Japan; and IRAP and the Data Hosting Certification Framework in Australia), there are also important technical differences and operational barriers that stand in the way of greater harmonisation of these standards and government assurance programs. Moreover, as critical sectors move toward greater cloud adoption, demand for assurance that cloud services meet heightened security standards continues to grow.

A more harmonised approach to cloud security requirements, leveraging of global cloud security standards (such as ISO 27017), and reciprocity of certification artifacts would increase security and resilience of digital infrastructure across the IPEF parties. It would also strengthen supply chains between IPEF markets and have a positive impact outside of those markets by providing a clear, harmonized set of cloud security practices and approaches to assurance for others to align with.

More broadly, promoting the use of modern, hyperscale public cloud services will support digital transformation in a secure and resilient way. Public cloud provides best-in-class security protection that is suitable in the vast majority of use cases, including in critical sectors. The modernisation of IT, underpinned by public cloud, is the most effective way of strengthening security across sectors.

5G and Trusted Telecommunications Networks.

5G and beyond communications technologies increasingly rely on cloud infrastructure. Compared with traditional 5G networks, cloud-based, software-defined networking is more efficient, scalable, and secure. IPEF countries can help ensure that regional regulations and procurement policies facilitate this shift to the cloud, which would stimulate a new generation of digital innovation on trusted networks.

IPEF countries should aim to develop common principles for 5G and 6G infrastructure. This would deliver benefits for IPEF parties, but also provide global leadership and likely be an inspiration for other countries' own trusted infrastructure development. We see four key areas where the IPEF could foster public-private collaboration to develop these common principles:

- **5G Security policy**: To be effective, 5G security policy should be as global as possible and built upon common standards, such as the ones developed by 3GPP and the ORAN Alliance. Policymakers should leverage existing compliance standards and certifications to enforce minimum security baselines, while ensuring that any new security requirements or schemes enable cloud-native 5G networks and associated technology to remain agile.

- **5G supply chains**: Policymakers should address 5G supply chains holistically through solutions that address each of the key challenges: continuity, transparency, efficiency, and security. Since shifting RAN functions from the edge to the cloud (or vice-versa) creates a different paradigm with a new set of challenges, governments should support the work of standards-setting organizations that include different stakeholders from diverse backgrounds. Governments should promote public-private partnerships to strengthen the security of open source software, particularly when used in critical functions.

- **5G standards:** All aspects of 5G technologies, networks and services are based on a comprehensive framework of standards derived through the work of experts in a myriad of standards-setting bodies and working groups. Standards are an important vehicle for international harmonization on technology, business, and policy considerations, which allow private companies to efficiently serve global markets. Additionally, standards development should maximize international collaboration and adoption rather than support national or regional barriers.

- **Spectrum**: Decisions taken around spectrum management will have a long-lasting impact on the evolution of wireless technology. A shared set of principles on spectrum management should strike the right balance between flexible spectrum usage and appropriate limitations and protections for some services. To foster innovation, it is important to avoid blocking wireless innovation by defining future usage based on the current technological state of the art. Specific areas could include incentivizing spectrum sharing by licensed operators and secondary users, reducing barriers in spectrum auctions, fostering digital inclusion through spectrum allocation that supports competitive and affordable connectivity with widespread network coverage, including in rural areas, and ensuring fairness and transparency in spectrum use and licensing decisions.

Submarine cables.

Submarine cables are a key component of digital infrastructure, and there should be a strong shared interest from governments in their protection. Given that multilateral discussions on this topic have resulted in only limited progress in recent years, the **IPEF could play a role in developing a focused agreement on submarine cable protection among participating governments.** This could pave the way for an agreement that could include additional governments beyond the IPEF.

4. Catalysing and Ensuring the Integrity of Efforts to Cut Carbon Emissions

We strongly support the IPEF's inclusion of a pillar encompassing decarbonisation. We suggest that one foundational element that IPEF parties should seek to achieve in this pillar is **the development of common approaches to carbon accounting.** It is difficult to fix what you cannot measure, and thus a focus on measurement can help catalyse and validate efforts to combat climate change.

Reliable measurement and accounting of greenhouse gas (GHG) emissions is critical to climate accountability and attribution. There must be a transparent and interoperable system to track, report, and compare GHG emissions and removals. To that end, Microsoft is participating in the Carbon Call hosted by ClimateWorks Foundation.[6] Participating organisations commit to the following: advance the development of more universal accounting methodological standards for companies, including links to national transparency reporting; enable the expansion of access to reliable GHG emissions and removal

[6] Lucas Joppa, *The Carbon Call: Working Together to Build Reliable Carbon Accounting for the Planet*, Microsoft on the Issues (Blog), Feb. 10, 2022, *available at* https://blogs.microsoft.com/on-the-issues/2022/02/10/carbon-call-sustainability-net-zero/; The Carbon Call, *available at* https://carboncall.org/the-carbon-call/.

data; and strengthen the interoperability of digital carbon accounting infrastructures. **IPEF partners could advance these efforts by endorsing the Carbon Call and taking steps to encourage companies in their jurisdictions to adhere to it**.

More generally, IPEF could be a forum for partners to discuss the role of data science and technology in supporting and enabling accurate carbon measurement and, ultimately, work toward convergent standards governing carbon accounting.

* * *

We appreciate the opportunity to provide feedback to DFAT as it develops plans for the Indo-Pacific Economic Framework. We encourage DFAT to continue to engage actively with the private sector as the IPEF initiative progresses. We look forward to continuing to partner with you and are happy to address any questions you may have relating to our submission.