Before the
U.S. Department of Commerce
Washington, D.C.

Request for Comments on the Indo-Pacific Economic Framework	Docket No. ITA-2022-0001

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

Pursuant to the request for comments published by the United States Department of Commerce in the Federal Register at 87 Fed. Reg. 13,971 (Mar. 11, 2022), the Computer & Communications Industry Association (CCIA) submits the following comments in response to the Commerce Department's Request for Comments on the Indo-Pacific Economic Framework (IPEF). CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms.[1] These comments complement those filed concurrently with the Office of the U.S. Trade Representative regarding trade negotiating objectives for the IPEF.

I. INTRODUCTION

CCIA is strongly supportive of the Administration's decision to pursue a comprehensive engagement strategy in the Indo-Pacific Region. Key to continued economic growth, national security, and U.S. competitiveness is a strong U.S. presence and enhanced cooperation with partners in the region.

The United States is at a significant disadvantage due to its absence from the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) that will advance trade in the Asia-Pacific Region. The United States is excluded from trade promotion enabled by the agreement, which has limited the strength of U.S. economic influence in the Asia-Pacific Region, at a time when regional partners are key to countering China's discriminatory practices and rising digital authoritarianism. Active engagement with our trading partners in the region will offset this imbalance, and a trade agreement and further economic cooperation with strong commitments would be a positive step forward to re-establishing U.S. leadership.

[1] For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more, visit www.ccianet.org.

These comments address the following issue areas identified in the Department of Commerce's request for comments: general negotiating objectives for the IPEF; digital and emerging technologies related issues; supply chain resilience-related issues; clean energy-related issues; tax-related issues; issues of particular relevance to small and medium-sized businesses that should be addressed in the negotiations; and other issues for consideration – encouraging good regulatory practices in digital regulations.

II. GENERAL NEGOTIATING OBJECTIVES FOR THE IPEF.

The United States should be ambitious in its negotiating goals to address as many access barriers to U.S. exports as possible in the Indo-Pacific Region, and secure binding rules and commitments from trading partners. As noted above, the United States is at a disadvantage by its absence in comprehensive regional trade agreements including the CPTPP. The U.S. should take advantage of the IPEF to address any shortcomings that absence in those agreements has created in terms of non-tariff barriers to trade.

The United States should pursue binding commitments with meaningful enforcement mechanisms and clear built-in review mechanisms to ensure that the IPEF continues to be durable and effective. There should not be broad exceptions that render commitments meaningless, such as the broad exceptions outlined in the Regional Comprehensive Economic Partnership (RCEP)[2] that limited the effectiveness of trade liberalization through trade agreements.[3] U.S. officials have noted that there will be flexibility within the structure of the IPEF, allowing countries to join certain pillars.[4] To the extent flexibility is needed within the IPEF, CCIA encourages the United States to allow for phased-in implementation of commitments rather than carve-outs.

As these negotiations are conducted, there should be measures taken to ensure transparency. The IPEF, as currently framed, is to be a multifaceted framework that aims to include trade commitments and other market access agreements, as well as other agreements on strategic cooperation among key partners, all taking place across U.S. agencies. Given the new

[2] Regional Comprehensive Economic Partnership text available at https://www.mofa.go.jp/policy/economy/page1e_kanri_000001_00007.html.

[3] RCEP's rules on prohibitions of localization measures and data flows contain broader exceptions and limitations that should not be replicated in U.S.-negotiated frameworks. *See* RCEP Art. 12.14, 12.15.

[4] *Bianchi: IPEF participants can join by pillar; U.S. will look for 'early harvests'*, INSIDE U.S. TRADE (Apr. 5, 2022), https://insidetrade.com/daily-news/bianchi-ipef-participants-can-join-pillar-will-look-%E2%80%98early-harvests%E2%80%99 (reporting statements made by Deputy U.S. Trade Representative Sarah Bianchi on the IPEF).

multi-structured approach, transparency will be even more important as compared to traditional trade negotiations. There should be readouts following each negotiation round or key engagements that inform stakeholders on topics being discussed and how parties seek to memorize commitments or agreements reached. Further, there should be meaningful opportunities for engagement by all stakeholders to address ongoing discussions as they occur. CCIA welcomes the Administration's commitment to inclusive engagement to ensure equitable and inclusive trade, and encourages Commerce to craft any IPEF pursuant to these principles.

III. DIGITAL AND EMERGING TECHNOLOGIES RELATED ISSUES.

The Indo-Pacific Region is a key digital market, where the number of Internet users is expected to grow to 3.1 billion by 2023.[5] As such, the digital economy pillar will be a critical component in the IPEF and participants should be ambitious in its goals in pursuing commitments and further economic cooperation on issues relevant to the digital economy.[6]

a. Enabling cross-border data flows and trust in digital services.

These negotiations present an opportunity to further enable digital trade and the U.S. should be ambitious in its negotiating objectives with respect to data flows and localization barriers. Cross-border data flows are critical to digital trade, and forced localization mandates make it difficult for U.S. exporters to expand into new markets. Studies have found that "for many countries that are considering or have considered forced data localization laws, local companies would be required to pay 30-60% more for their computing needs than if they could go outside the country's borders."[7] Another study found that the impact of recently proposed or enacted data localization legislation on GDP is "substantial" in seven countries.[8] Analysis from the OECD has revealed an increasing level of restrictiveness for digitally-enabled services in part due to restrictions on cross-border movement of data.[9] Cross-border data flows are the lifeblood

[5] CSIS, *Filling In the Indo-Pacific Economic Framework* (Jan. 2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220126_Goodman_Indo_Pacific_Framework.pdf.

[6] *See also* Industry Letter to Ambassador Tai, Sep. 10, 2021, *available at* https://www.itic.org/documents/trade/LettertoAmb.TaionPacificDigitalTradeAgreements_Final09102021.pdf.

[7] Leviathan Security Group, *Quantifying the Cost of Forced Localization* (2014), *available at* https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

[8] Matthias Bauer *et al.*, *The Costs of Data Localization* (ECIPE 2014), *available at* http://www.ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf (finding that the GDP was reduced in the following countries with data localization policies: Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%), and Vietnam (-1.7%)).

[9] OECD Services Trade Restrictiveness Index: Policy Trends up to 2020, *available at* https://issuu.com/oecd.publishing/docs/oecd-stri-policy-trends-up-to-2020?fr=sNmVlNzYxOTI3Mw.

of global digital trade and by extension the array of industries that increasingly rely on the Internet to compete in the global marketplace. In the U.S. the productivity gains and efficiencies enabled by data flows have boosted the economy by hundreds of billions of dollars.[10]

With an uptick in data-related barriers in recent years, clear rules are critical to ensure that any restrictions are consistent with existing international obligations and are targeted in a manner that does unreasonably limit legitimate cross-border trade.[11] Policies that restrict data flows, either directly through explicit data and infrastructure localization requirements, or indirectly for national security or other purposes, negate the productivity gains and efficiencies enabled by Internet platforms and cloud computing.

The United States should pursue rules that prohibit governments from interfering with data flows or the exchange of information online. Specifically, rules should prohibit governments from imposing data localization or local presence requirements on data controllers or processors, as well as linking market access and/or commercial benefits to investment in or use of local infrastructure. To the extent possible, these prohibitions should apply to both explicit and indirect measures to keep data in a particular country.

Trust in the cross-border delivery of these services is critical. Without adequate privacy protections and security in digital communications, governments may continue to enact restrictions on cross-border services citing perceived risks. Privacy and consumer protections and trade rules should work in tandem to further goals of initiatives including the "data free flow with trust" launched by heads of governments under Japan's G20 leadership in 2019.

To that end, IPEF countries should prioritize development of national privacy legislation that sets clear rules on the use of personal data domestically, promote the adoption of bilateral and multilateral agreements on government access to data such as those being pursued by the OECD[12], and commit to codify into domestic law protections for valid basis for transfer of personal data such as the APEC Cross-Border Privacy Rules.

---

[10] Joshua Meltzer, *Data and the Transformation of International Trade*, BROOKINGS INSTITUTION (Mar. 6, 2020), https://www.brookings.edu/blog/up-front/2020/03/06/data-and-the-transformation-of-international-trade/.

[11] Examples of these barriers are documented in CCIA's Comments to USTR for the preparation of the annual National Trade Estimates Report, available at https://www.ccianet.org/wp-content/uploads/2021/10/CCIA-Comments-2022-National-Trade-Estimate-Reporting.pdf.

[12] *See* OECD, Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy (Dec. 2020), https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm.

b. Prohibition on customs duties for electronic commerce.

Imposing customs requirements on purely digital transactions creates significant and unnecessary compliance burdens on nearly all enterprises, including small and medium-sized enterprises (SMEs). There would need to be several requirements created that would accompany such an approach, many of which would be extremely difficult to comply with. For instance, data points required for compliance include the description of underlying electronic transfer, end-destination of the transmission, value of transmission, and the country of origin of the transmission — all of which do not exist for most electronic transmissions, especially in the cloud services market.

The moratorium on imposing customs duties for electronic transmissions[13] has been key to the development of global digital trade and shows the international consensus with respect to the digital economy, reflected in the number of commitments made in free trade agreements among multiple leading digital economies. Permanent bans on the imposition of customs duties on electronic transmissions are also a frequent item in trade agreements around the world. This includes, but is not limited to, Article 14.3 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[14] Article 19.3 of the U.S.-Mexico-Canada Agreement (USMCA),[15] and Article 8.72 of the EU-Japan Economic Partnership Agreement.[16]

The United States should continue to advocate for the permanent ban on the imposition of customs duties on electronic transmissions in the IPEF, and continue to discourage countries from including electronic transmission in their domestic tariff codes.

c. Online content regulations and addressing state-censorship practices.

Censorship and denial of market access for foreign Internet services has long been the case in restrictive markets like China, but it is becoming increasingly common in emerging digital markets as well as some traditional large trading partners, and accomplished through different tools and methods. The U.S. International Trade Commission released its report on

[13] The 2nd Ministerial Conference of the World Trade Organization in 1998 produced the Declaration of Global Electronic Commerce which called for (1) the establishment of a work program on e-commerce and (2) a moratorium on customs duties on electronic transmission. The moratorium has been renewed at every Ministerial since that time.

[14] Final Text of Comprehensive and Progressive Agreement for Trans-Pacific Partnership, signed Mar. 8, 2018, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

[15] Final Text of U.S.-Mexico-Canada Agreement, signed Nov. 30, 2018, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.

[16] Final Text of Agreement Between EU and Japan for Economic Partnership, http://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf#page=185.

foreign censorship policies in January 2022 and detailed how extensive these practices have become, noting that:

> The consequences of censorship-related policies and practices can be significant for U.S. firms, especially U.S.-based content producers and digital services firms, as they may restrict trade, impede market access, increase operational costs and reputational risks, or discourage foreign direct investment.[17]

IPEF partners should work together to address rising digital authoritarianism and state-censorship practices that pose threats to the open Internet and freedom of expression around the world. Because the business community has a limited technical capacity to assess and respond to interference with cross-border flow of services, products, and information by nation-states, allied governments have a critical role to play in partnering with technology companies and leading in the defense of Internet freedom and open digital trade principles.

Countries should affirm commitments under Article 19 of the International Covenant on Civil and Political Rights as they apply to defending free expression online. The IPEF should include clear commitments to refrain from blocking or restriction access to lawful online content, digital services, and infrastructure underlying Internet delivery.

Government-imposed restrictions of digital services and online content can take multiple forms, and the risks associated with each method or regulatory framework providing for censorship methods can vary greatly.[18] For example, some types of content restrictions may be reasonable and legally permissible in certain contexts, but may result in overbroad removals of user speech if attached to filtering or monitoring requirements. Other trade concerns arise where content policies are not applied equally to both domestic and foreign websites. Furthermore, an increasing number of content restrictions do not comply with World Trade Organization (WTO) principles of transparency, necessity, minimal restrictiveness, and due process to affected parties.

Internet services recognize the importance of ensuring user trust and safety and have significantly increased resources to ensure that their services remain spaces for free expression,

---

[17] U.S. INT'L TRADE COMM'N, *Foreign Censorship, Part 1: Policies and Practices Affecting U.S. Businesses* (Feb. 2022), *available at* https://www.usitc.gov/publications/332/pub5244.pdf at 21.

[18] *See,* U.S. INT'L TRADE COMM'N, *Foreign Censorship, Part 1: Policies and Practices Affecting U.S. Businessess*; Testimony of the Center for Democracy & Technology Before Senate Finance Committee, *available at* https://cdt.org/wp-content/uploads/2022/03/CDT-Emma-Llanso-Senate-Finance-Committee-Testimony-15-March-2022.pdf at 5-6; Comments of CCIA, U.S. ITC Investigation No. 332-585: Foreign Censorship Part 1: Policies and Practices Affecting U.S. Businesses, https://www.ccianet.org/wp-content/uploads/2021/07/CCIA-Comments-USITC-Censorship-Trade-Barriers.pdf.

that users comply with their terms of service, and that illegal and harmful content that violates their terms of service is identified and removed. But the expanding array of emerging content regulatory frameworks often have the impact of making it harder, rather than easier, for U.S. Internet companies to strike the right balance between promoting free expression and taking action against dangerous content.[19] Rules should be consistent, clear, and work for companies of all stages of development to encourage the export of Internet services. Doing so enables Internet exporters to establish comprehensive practices to proactively address harmful content and behavior that violates terms of service, while enabling open discourse online. These commitments should work in tandem with commitments on good regulatory practice and additional global standards on content removal that ensure due process, oversight, and accountability.

d. Non-discriminatory approach to cybersecurity certification.

Cybersecurity is essential as countries across the Indo-Pacific region work to advance their digital transformation goals for their government, their economies, and their societies. However, there is a growing trend of governments using cybersecurity certification requirements to discriminate against foreign technology companies, particularly in the cloud sector.

Some countries in the Indo-Pacific region require government agencies, state-owned entities, and even critical infrastructure companies to select only from vendors with a national cybersecurity certification, which foreign companies are unable to meet. As part of the digital component in the IPEF, the United States should secure binding commitments from trading partners to adopt a risk-based approach to cybersecurity certifications, as well as to treat foreign companies no less favorably than local companies in the cloud sector, and specifically to agree that cybersecurity certification eligibility should not be conditioned on nationality of ownership of a cloud company seeking such certification.

e. Securing digital communications and devices.

Providers of digital devices and services have sought to improve the security of their platforms through the deployment of technologies that safeguard the communications and commercial transactions that they enable. Strong encryption has been increasingly enabled on now-ubiquitous smartphones and deployed end-to-end on consumer-grade communications

[19] Examples of these barriers are documented in CCIA's Comments to USTR for the preparation of the annual National Trade Estimates Report, available at https://www.ccianet.org/wp-content/uploads/2021/10/CCIA-Comments-2022-National-Trade-Estimate-Reporting.pdf.

services and browsers. Encrypted devices and connections protect users' sensitive personal and financial information from bad actors who might attempt to exploit that information.

Many countries, at the behest of their respective national security and law enforcement authorities, have passed laws that mandate access to encrypted communications. Often the relevant provisions are not explicit, but mandate facilitated access, technical assistance, or compliance with otherwise infeasible judicial orders. Other versions require access to or transfer of source code as a condition of allowing technology imports. Other recent measures impose "traceability" requirements that undermine encryption measures, like those included in India's 2020 IT Act (Intermediary Rules) Amendments.[20] Such exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and implement.[21] Companies already operating in countries that have or are considering anti-encryption or source code access laws will be required to alter global platforms or design region-specific devices, or face fines and shutdowns for noncompliance. Companies that might have otherwise expanded to these markets will likely find the anti-encryption or facilitated access requirements to be barriers to entry.

The United States should continue efforts to promote regulatory cooperation and international standards for securing products and services. The IPEF should contain commitments to promote encrypted devices and connections. Specifically, the IPEF should prevent countries from compelling manufacturers or suppliers to use a particular cryptographic algorithm or to provide access to a technology, private key, algorithm specification, or other cryptographic design details. Similarly, IPEF should prohibit governments from conditioning market access, with appropriate exceptions, on their ability to demand access to cryptographic keys or source code. Additionally, the IPEF should include commitments for partners to pursue risk-based cybersecurity measures, as it is the more effective approach in comparison to prescriptive regulation. IPEF partners should pursue cooperative approaches to cybersecurity and incident responses, including sharing of information and best practices.

[20] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, *available at* https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021.

[21] Harold Abelson, et al., Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, MIT Computer Science and Artificial Intelligence Laboratory Technical Report, July 6, 2015, http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

f. Fostering innovation in emerging technologies.

Emerging technologies such as artificial intelligence (AI) and machine learning, as well as quantum computing, increasingly impact cross-border trade, and trade rules increasingly govern the development and growth of these technologies. To continue to use and export AI and other emerging technologies, businesses and users need a framework that allows them to move data and infrastructure safely across borders while ensuring that other countries will not misuse legal systems to impede the growth of new technologies. This will enable use of emerging technologies in addressing global challenges such as public health, humanitarian assistance, and disaster response.

IPEF partners can facilitate the responsible cross-border growth of AI technologies by committing to enabling cross-border data flows and removing localization requirements; encouraging governmental investment in and release of open data; identifying and sharing best practices for the responsible use of AI; cooperation and public-private collaboration on AI; and the adoption of innovation-oriented copyright rules that enable machine analysis of data. In addition, to ensure substantive convergence and avoid the potential for discriminatory outcomes, the U.S. and its Indo-Pacific trading partners should agree to avoid adopting any measures that violate national treatment rules or give less favorable treatment to AI products or applications than they give to like products or applications without an AI component.

As a matter of good regulatory practice, the development and implementation of AI regulations should include: adopting a risk-based approach, including transparent processes for assessing, managing, and mitigating risks associated with specific AI applications; assessing whether potential risks can be mitigated or addressed using existing instruments and regulatory frameworks; considering whether any new or proposed regulation is proportionate in balancing potential harms with economic and social benefits; employing risk management best practices, including considering the risk-substitution impact of a specific AI application against a scenario where that application has not been deployed but baseline risks remain in place; and promoting the development of voluntary consensus standards to manage risks associated with AI applications in a manner that is adaptable to the demands of dynamic and evolving technologies.

IPEF countries should work together to facilitate research and development of new applications of AI to address shared challenges; facilitate dialogues among all stakeholders

including governments, civil society, academic, and the private sector on best regulatory practices; and pursue joint discussions on the responsible and ethical use of AI.

g. Encouraging adoption of cloud computing services.

Cloud computing services will play a key role in the economic future of the Indo-Pacific region and beyond, including with respect to the digitalization of government and private-sector operations and services. Cloud computing enables businesses and governments to access powerful computational resources, storage and highly-secured IT infrastructure and services. However, cloud service providers are facing increasing market access and procurement barriers in the Indo-Pacific region.

Within the IPEF, the United States should pursue commitments from participations to reduce barriers and ensure non-discriminatory treatment of foreign cloud service providers. This includes commitments to (1) provide full access and non-discriminatory treatment for cloud services and service providers based in an IPEF country, including for any government procurement; (2) use open tendering procedures for the procurement of cloud services or digital services, and (3) adherence to internationally-recognized standards, including the ISO 2700 family of information security management standards, in cloud services certification procedures, to support privacy and security and encourage interoperability across markets.

h. Addressing technical barriers to trade.

The Administration has limited discussion of technical barriers to trade under the IPEF to the agriculture sectors. However, U.S. technology exporters face a growing number of non-tariff measures such as technical regulations, conformity assessment practices, and standards-based measures. Adoption of global standards is critical to ensuring regulatory coherence and avoiding country-specific standards that deter market entry. Some U.S. cloud service providers (CSPs) have been unable to serve the public sector due to onerous security certification requirements that deviate from internationally accepted standards and make it impossible for CSPs to comply without creating a market-unique product, including physically segregating facilities for exclusive use for government-owned customers and onshoring data. The adoption of country-specific standards creates de facto trade barriers for U.S. companies and raises the costs of cutting-edge technologies for consumers and enterprises.

In the IPEF, the United States should (1) pursue commitments like those outlined in USMCA Chapter 11 on addressing technical barriers to trade; and (2) pursue commitments to

follow good regulatory practices as detailed in Section VIII of these comments in the development on of standards, regulations, and conformity assessment procedures for services.

i. Non-discriminatory approach to cybersecurity certification.

Cybersecurity is essential as countries across the Indo-Pacific regions work to advance their digital transformation goals for their government, their economies, and their societies. However, there is a growing trend of governments using cybersecurity certification requirements to discriminate against foreign technology companies, particularly in the cloud sector. As noted above, some countries in the Indo-Pacific region require government agencies, state-owned entities, and even critical infrastructure companies to select only from vendors with a national cybersecurity certification, which foreign companies are unable to meet. As part of the digital component in the IPEF, the United States should secure binding commitments from trading partners to adopt a risk-based approach to cybersecurity certifications, as well as to treat foreign companies no less favorably than local companies in the cloud sector, and specifically to agree that cybersecurity certification eligibility should not be conditioned on nationality of ownership of a cloud company seeking such certification.

j. Following global practices on Internet access and interconnection policies.

Countries participating in the IPEF should work to protect the interoperable and interconnected nature of the global Internet architecture that enables cross-border data flows, support principles of non-discrimination and market access to telecommunications networks, and enable stakeholders to negotiate the nature of services to be delivered across the network on a commercial basis.

There are recent legislative proposals that have threatened this approach by attempting to regulate interconnection charges between Internet service providers (ISPs) and content providers, and risk creating significant barriers to cross-border data flows by taxing the delivery of online content.[22] Globally, the business practice on Internet interconnection is for content providers and ISPs to enter into agreements through autonomous negotiations. An OECD paper found that 99.5% of interconnections are made without written contracts, and "the Internet model of traffic exchange has produced low prices, promoted efficiency and innovation, and attracted the

[22] See HUDSON INSTITUTE, *A Harmful Step for the Internet in Korea* (Jan. 11, 2022), https://www.hudson.org/research/17470-a-harmful-step-for-the-internet-in-korea; *see also* Son Ji-hyoung, *GSMA to press streaming platforms on network cost-sharing: KT CEO*, KOREA HERALD (Mar. 2, 2022), http://www.koreaherald.com/view.php?ud=20220302000769.

investment necessary to keep pace with demand." IPEF countries should ensure that Internet-based telecommunications service providers seeking to exchange of traffic with content and application providers, and vice versa, are able to negotiate with the other party on a voluntary and commercial basis, and that access to domestic telecommunications network should be on reasonable and non-discriminatory terms.

IV. SUPPLY CHAIN RESILIENCE-RELATED ISSUES.

The IPEF comes at a critical time as the COVID-19 pandemic has made clear the weakness and limitations of the existing global supply chain. The Administration has taken a number of critical steps in identifying these limitations, and the Department of Commerce's work in this area is welcomed. The United States should incorporate these lessons learned into the IPEF, and commit to further engagement with partners to establish programs to increase resiliency.

One area of focus for the IPEF discussions should be how to more efficiency get facilitates back online that are necessary for global supply chains. When facilities that produce a key product or input are closed, the unavailability of key components curtails the production of downstream products and escalate delays. Lack of sufficient planning, poor organization, lack of technical expertise or relevant managerial capacity, and lack of resources are all reported barriers to re-opening these facilitates.

IPEF countries can address these challenges by (1) setting up an institutional framework within both the U.S. government and that of regional partners to rapidly identify and mitigate shutdowns of supply chain-critical facilities resulting from public health emergencies, natural disasters, or other external events; (2) providing capacity building to governments in the skills necessary to establish rapid-reaction mechanisms within their domestic frameworks; and (3) establishing a network and mechanism for the rapid deployment of material aid necessary to get facilities back online.

V. CLEAN ENERGY-RELATED ISSUES.

The IPEF framework should enable companies operating throughout the region to achieve renewable energy goals. Participants should work to open up markets for U.S. and foreign investors in renewable energy, and reduce regulatory barriers for investment in renewable energy.

However, in many markets, regulations favor legacy energy sources and serve as barriers to building new renewable energy projects, leaving companies with no choice but to use more carbon intensive power sources. The IPEF presents an opportunity for governments to remove regulatory barriers to foreign investment and construction of renewable energy plants.

Resource recovery of used technology products can also help in reaching climate-related goals. The use of raw materials recovered from these used products can help reduce the need for mining virgin materials, reduce waste, and can also enhance supply chain resiliency by capitalizing on the supply of critical materials already embedded in consumer devices. A current barrier to wider adoption of resource recovery practices is international rules that limit the cross-border movement of used consumer devices and the resources recovered from them. IPEF partners should use this platform to explore options to reduce these barriers, and explore possibilities around establishing "resource recovery lanes" among trusted partners.

VI. TAX-RELATED ISSUES.

International trade requires a consistent and predictable international tax system, and tax measures play a significant role on global competitiveness of U.S. companies.

On October 8, 2021, the Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalization of the Economy was released outlining the agreed-upon framework for global corporate tax reform.[23] Pursuant to this commitment, all countries that have agreed to this framework cannot introduce any new unilateral measures and CCIA urges countries to abandon any national plans to implement national digital taxes and encourages policymakers to continue work on swift implementation of the global framework.

IPEF partners should continue efforts to implement this multilateral solution, and should commit to avoid any digital taxation measures that are discriminatory in nature and contravene long-standing principles of international taxation.

[23] OECD G20/Base Erosion and Profit Shifting Project, Statement on a Two-Pillar Solution to Address to the Tax Challenges Arising from the Digitalization of the Economy (Oct. 8, 2021), https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf (stating "The Multilateral Convention (MLC) will require all parties to remove all Digital Services Taxes and other relevant similar measures with respect to all companies, and to commit not to introduce such measures in the future. No newly enacted Digital Services Taxes or other relevant similar measures will be imposed on any company from 8 October 2021 and until the earlier of 31 December 2023 or the coming into force of the MLC. The modality for the removal of existing Digital Services Taxes and other relevant similar measures will be appropriately coordinated.").

VII. ISSUES OF PARTICULAR RELEVANCE TO SMALL AND MEDIUM-SIZED BUSINESSES THAT SHOULD BE ADDRESSED IN THE NEGOTIATIONS.

Digital services enabled businesses of all sizes and across different industries to continue operations throughout the COVID-19 pandemic, and access to digital tools can help SMEs overcome export challenges. The IPEF should have a dedicated work stream focused on helping SMEs throughout the Indo-Pacific region continue to grow and reach new markets, working to establish dialogue among interested stakeholders to identify ways and share best practices on how the digital economy can facilitate SMEs. Additionally, IPEF countries should commit to rules that ensure that licensing and registration procedures for exporters are simple, fair, and transparent. SMEs would also benefit from prohibition of local presence requirements.

VIII. OTHER ISSUES FOR CONSIDERATION - ENCOURAGING GOOD REGULATORY PRACTICE IN DIGITAL REGULATIONS.

The global Internet economy is at a pivotal moment in its development, one in which the openness and free exchange that has led to unprecedented growth and opportunity are now challenged by protectionist inclinations on the part of many trading partners, including some traditional U.S. allies. Countries continue to move fast to introduce new regulatory frameworks on data governance, and seek to craft rules on the development of emerging technologies. Industry reports new (1) sectoral regulations that target specific U.S. firms rather than business conduct generally, (2) restrictive data governance policies that mandate localization and restrict cross-border delivery of services, and (3) a regulatory environment that disadvantages foreign firms by restricting digital activities in the region and/or imposing local residency requirements.

As new proposals are introduced around the world, countries should commit to following good regulatory practice and work together to ensure that regulations to not have unintended impacts. International regulatory cooperation is an important tool for improving regulatory quality, reducing the likelihood of creating trade barriers or unnecessary regulatory differences, aligning regulation with shared principles and values, avoiding unintended consequences or conflicts with broader foreign policy objectives, building trust and expertise among regulators, and deepening understanding of trends in regulatory governance to inform current and future approaches to policymaking.[24]

[24] *See* CCIA Recommendation on U.S.-EU Trade & Technology Council: Incorporating Stakeholder Input within International Regulatory Cooperation, https://www.ccianet.org/wp-content/uploads/2021/09/CCIA-TTC-Recommendations-Incorporating-Stakeholder-Input-within-International-Regulatory-Cooperation-2021.pdf.

The United States should use the IPEF to pursue governing principles of the digital economy that ensure that regulations should be non-discriminatory and principles-based, made pursuant to a transparent regulatory process, ensure due process to those affected, and include adequate safeguards to reduce the impact of any unintended consequences.

IX. CONCLUSION

CCIA supports the Administration's efforts to pursue a comprehensive strategy for engagement in the Indo-Pacific Region. Industry appreciates the opportunity to share its views on how the IPEF can lead to continued economic growth and U.S. competitiveness in the region through enhanced cooperation with key partners.

April 11, 2022

Respectfully submitted,

Rachael Stelly
Senior Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, D.C. 20001