ITI's Proposal for Collaboration in the
Indo-Pacific Economic Framework:

The Trusted Digital
Partnership Program

May 2022

ITI
Promoting Innovation Worldwide

ITI's Proposal for Collaboration in the Indo-Pacific Economic Framework: **The Trusted Digital Partnership Program**

ITI encourages the Department of Commerce to address digital issues that implicate trust in a holistic manner. In particular, the United States can incentivize partner economies to adopt digital trade-facilitative regulatory policies by proposing a Trusted Digital Partnership Program that will encourage investments by technology companies and facilitate business partnerships. Governments that implement complementary regulatory policies, norms and standards would set preconditions for businesses in the region to share data and build intertwined supply chains for technology goods and services more easily.

Both technology businesses and consumers value trust in their relationships in sharing data and developing products and services. Governments can adopt laws, regulations, norms, and use standards that build trust in their legal and business environments. Companies that are governed by those laws, regulations, and policies will be more trusted; and countries that provide a legal and policy ecosystem that is aligned to and interoperable with other trusted jurisdictions will encourage more cross-border investment and business cooperation, particularly in the technology sector.

This approach would complement efforts in the Fair and Resilient Trade module to obtain legally enforceable commitments to ensure cross-border data flows and the provision of digital services across borders. In concert with such provisions, this approach would assert U.S. leadership in the operationalization of the concept of "Data Free Flow with Trust (DFFT)" in a manner that comports with broader administration priorities. Governments' commitments on trusted digital policies, rather than being legally enforceable, would provide powerful incentives for IPEF participants to align themselves with them by encouraging investment and economic growth, enabling access to targeted U.S. aid and technical assistance, and enabling increased availability of trusted ICT goods and services to counter shared resiliency challenges.

ITI encourages the United States to propose a two-phase Trusted Digital Partnership Program module (or set of modules) consisting of 1) mutual pledges to establish and maintain trusted digital policies, and 2) deployment of capacity building and technical assistance to achieve these policy commitments and facilitate transnational public-private economic partnerships.

Below, we elaborate further in details of what the two-part Program could include:

Part I: Adoption of Trusted Government Digital Policy Commitments

Governments can establish a trusted legal and policy environment by pledging to abide by the following 12 procedures and practices:

1 **Promote the Rule of Law.** Maintain an independent judiciary, with courts and tribunals that follow consistent and transparent procedures and legal processes without being subject to political interference.

2 **Ensure legal limits on government access to personal data.** Demonstrate respect for the rule of law by establishing clear legal or judicial limitations on the proportionate exercise of power by the government to access personal data for legitimate law enforcement or national security purposes and provide companies with transparent processes for challenging government requests for personal data.

3 **Demonstrate commitment to human rights.** Observe international human rights commitments, including a free media, and absence of censorship and arbitrary detentions based on technological surveillance, or other actions contrary to accepted human rights practices and international norms.

4 **Cooperate on government access to digital information.** Develop efficient and innovative mechanisms for issuing and responding to cross-border requests for digital information for law enforcement or national security purposes. This includes enhancing the speed and operation of Mutual Legal Assistance Treaties (MLATs) to make them effective in the digital age, as well as drawing on national or regional legislation to develop approaches to cross-border lawful access requests that are transparent, interoperable, and grounded in the rule of law.

5 **Provide strong privacy protections.** Adopt and maintain policies that promote strong privacy protections and data security, such as through data minimization, privacy by design, and encryption. This includes effective individual control rights, including the right to access, correct, port, delete, consent, and object to the use of personal data. Privacy and personal data protection frameworks should offer multiple grounds for legal processing, including consent, legitimate interests of the data controller, contractual necessity, fulfillment of a legal obligation, and protection of public health, safety and security or other vital national interests.

6 **Implement robust mechanisms for cross-border data transfer.** Ensure the availability of transparent, non-discriminatory legal mechanisms for the cross-border transfer of personal data. In particular, governments should adopt and maintain at least one but ideally multiple tools for data transfers, beginning with binding multi-jurisdictional framework agreements, and including mechanisms such as model contract clauses, approved intra-company rules, certifications based on international standards, independent seals, or the accountability mechanisms of national law or regional or multilateral agreements.

7 **Avoid restrictions on non-personal data.** Governments should refrain from restricting the cross-border movement of non-personal data, including machine-to-machine communications. Governments should seek instead to enable access to and use of open government data and utilize voluntary data sharing frameworks to facilitate the use by public and private entities and other organizations of non-sensitive, non-personal data in pursuit of research, academic, or scientific objectives, or initiatives in the public interest.

8 **Promote ethical corporate behavior and counter corruption.** Establish laws against corruption and theft of intellectual property, while promoting ethical corporate behavior. Enhance transparency of ownership for large companies and promote public financial accounting standards consistent with international commercial standards.

9 **Promote development and adoption of international standards for digital services and new technology.** Reinforce and supplement existing multilateral commitments to promote the participation of partner countries in the development and use of international standards and ensure that governance of digitally-enabled services and new technologies, such as future generations of wireless communication and artificial intelligence, are grounded in industry-driven international standards.

10 **Enable a strong ICT workforce pipeline.** Support and expand programs that attract, educate, and train the ICT workforce as a necessary precondition for advanced manufacturing and development of ICT products, digital services, and related investment.

11 **Establish transnational public-private partnerships for research, development and commercialization among Trusted Digital Partnership Program countries.** Cooperation among trusted countries' governments, academic and research institutions, and private sector technology companies will produce leading edge innovation and economic growth. Governments should establish mechanisms for collaboration on technology research, development and commercialization with dedicated financing, seeking the commitment of both public and private funding and the involvement of international partners.

12 **Take a risk-based approach to managing cybersecurity risk.** As cybersecurity threats continue to evolve, it is increasingly important that countries determine how to identify, manage, and respond to cybersecurity risks. Countries should pursue risk-based approaches grounded in international, consensus-based standards to managing and mitigating cybersecurity risk. Leveraging this type of approach will help to facilitate innovation, while ensuring that cybersecurity regulation is not overly prescriptive and does not result in fragmentation.

Part II: Support Implementation through Technical Assistance and Capacity Building

The United States government should leverage existing and establish new technical assistance and capacity building programs to help countries that sign up for the above commitments to implement trusted government digital policies. Efforts could be conducted on a regional or bilateral basis. The Digital Connectivity and Cybersecurity Partnership is a good example of a technical assistance and capacity building program that could be oriented to support meeting the commitments of the Trusted Digital Partnership Program. Other opportunities for such technical assistance and capacity building include:

Cybersecurity

Adopting risk-based frameworks and ensuring effective and efficient incident reporting regimes. Leveraging the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the USG can provide technical assistance to governments in the region to enact legal and regulatory tools to advance voluntary approaches to cybersecurity risk management consistent with the framework, including to integrate cyber incident reporting into those activities. NIST, U.S. Department of Homeland Security (DHS) and the State Department could all participate. There is strong interest and awareness about the benefits of the NIST Framework, and NIST has already undertaken some outreach and awareness efforts. Scaling this up can provide early wins and benefit all stakeholders.

Artificial Intelligence (AI)

Facilitating the development of and reliance on international standards. Recognizing that challenges related to AI transparency, bias, and risk management are of the highest interest to policymakers, the USG could convene countries making the trusted policies pledge to establish a government working group that would facilitate monitoring and participation in the OECD's AI Policy Observatory, Global Partnership on AI (GPAI) and other government-led initiatives that are developing normative frameworks for AI. USG could also partner with the American National Standards Institute (ANSI) to support further ANSI collaboration with its peer national standards bodies in the countries making the trusted policies pledge to engage in the development and use of AI standards, such as those developed by the ISO-IEC's Joint Technical Committee (JTC) 1. The ultimate goal would be to ensure that the countries making the pledge are able to use these standards to support their governance and regulatory structures for AI and ensure that they are first movers in the deployment of AI use cases. As part of such efforts, and to proselytize innovation-facilitative elements of the United States' approach to standardization, the USG could consider developing, supplementing, and reorienting

funding for technical assistance programs and public-private partnerships (e.g., The Standards Alliance) to provide robust and meaningful support for partner countries' participation in the development and use of international standards. Such efforts would have the added benefit of serving as a counterweight to other governments' efforts to promote the adoption of country- or region-unique standards, which disadvantage U.S. firms and risk technological fragmentation.

Edge Computing

Enabling leadership on edge computing applications though public-private partnerships. As 5G infrastructure (and eventually 6G technology) is deployed over the next few years, the use cases and applications for this telecom infrastructure will generate massive economic value. The infrastructure is becoming increasingly virtualized (software-driven) and will push computer processing to the edge, closer to the user. This will reduce latency and the cost of data-intensive computing applications – ranging from autonomous vehicles, logistics, health care and education to smart cities and advanced manufacturing. The USG can establish public-private partnerships with countries making the pledge to conduct advanced research and deployment of use cases. Cloud computing companies will be key players in virtualization and edge computing along with the traditional telecom operators and equipment manufacturers. Those companies along with companies operating in the vertical applications could be incentivized by joint U.S. and foreign government funding to commercialize use cases. The financing could take the form of lending by the U.S. Export-Import Bank and U.S. Development Finance Corporation, and technical assistance grants from the U.S. Trade and Development Agency.

ITI

Promoting Innovation Worldwide

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. We promote public policies and industry standards that advance competition and innovation worldwide.