ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

March 24, 2022

Ms. Diane Farrell
Deputy Under Secretary for International Trade
U.S. Department of Commerce
1401 Constitution Ave NW, Washington, DC, 20230

Re: ITIF Submission: Request for Comments on the Indo-Pacific Economic Framework (ITA-2022-0001)

Dear Ms. Farrell,

Please find below the Information Technology and Innovation Foundation's (ITIF) submission to the Department of Commerce's inquiry (docket no. ITA-2022-0001) into the Indo-Pacific Economic Framework (IPEF). The submission starts with a contents page and a summary of key recommendations, before providing a detailed description and analysis of each recommendation/issue.

Please let me know if you or your team have any questions.

Sincerely,

Nigel Cory
Associate Director, Trade Policy, The Information Technology and Innovation Foundation
Email: ncory@itif.org

CONTENTS

SUMMARY OF KEY RECOMMENDATIONS

Global Data Flows, Privacy, and Governance

- The United States should build data, digital, and technology processes and outcomes at IPEF that define the type of open, rules-based, and interoperable governance it wants to see in the global digital economy. In doing so, it would reject the perspective (mainly European) that harmonization—that there is a one-size fits all approach to data and technology governance—is the best approach to address global data and technology issues.
- The United States should explicitly reference and articulate the principle of accountability in regards to data governance—that privacy and other legal responsibilities move with the data.
- The United States should explicitly reference and articulate the principle of interoperability, such that data is still able to flow between different privacy regimes, and countries' data protection rules flow with it. An interoperable system would focus on "global protections through local accountability."
    - For example, IPEF partners should ensure outcomes explicitly allow for multiple different legal mechanisms to transfer personal data (similar to what Chile-New Zealand-Singapore did in their Digital Economy Partnership Agreement).
- The United States should include carefully designed "conditional linkages" in IPEF between various commitments, provisions, and programs within each (and potentially between) the four buckets, such that it does not scare Indonesia and Vietnam away, but incentivizes them to join and engage in good faith cooperation (absent the America's ability to make market access concessions).
    - To add value to existing agreements, it is key that IPEF move Indonesia, India, and Vietnam closer to the U.S. approach to data and digital trade (and that of Australia, Japan, New Zealand, and Singapore). Even just getting Indonesia and Vietnam engaged would be a win.
    - In parallel, the United States should build out the club of ambitious countries on digital issues such as to create a clearer incentive for these potentially problematic partners to join.
    - The United States should use a flexible approach, with connected conditionality, perhaps over an extended period of time, to encourage those members with problematic policies to move toward signing up to and joining ambitious provisions and programs.
    - The United States should make access to any preferential financing and technical capacity building, training, and other digital economy and advanced technology programs by the U.S. National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI), or USAID, contingent on genuine, good faith engagement on the full range of digital issues and rules.
        - To do this, the United States needs to better align U.S. development assistance with the commercial, trade, and strategic goals central to IPEF's digital and technology objectives and make access to ongoing and new programs contingent upon IPEF engagement.

    - The United States should use core IPEF partners (like Australia, Japan, and Singapore) as trusted intermediaries to engage with these countries given they may get a different reception. Indonesia and Vietnam are familiar with USTR's perspective. Along with the carrot, the United States could ask these trusted intermediaries to suggest to Vietnam that they may consider launching a CPTPP-based dispute case (given its use of data localization) if it fails to join IPEF and engage in genuine, good faith cooperation.
- New digital trade rules are definitely needed to prohibit and roll-back the growing range of digital barriers to trade, but these are insufficient on their own to future-proof trade frameworks so that firms can engage in seamless cross-border digital trade and innovation. U.S. policymakers must build-in regulatory cooperation with likeminded trading partners to ensure the early and ongoing alignment in how they govern data and new digital technologies.
    - Australia, Chile, New Zealand, and Singapore-style digital economy agreements show how truly modern trade agreements are as much about pursuing a model for digital governance that is international and interoperable as it is about agreeing on new, binding trade law provisions. It's as much about the regulatory engagement and cooperation as it is about new digital trade rules.
    - The United States should get respective agencies to review and revise existing regulatory cooperation with IPEF partners and determine whether new MOUs and other agreements are needed. The Department of Commerce would need to work with other agencies to get them to buy into new regulatory cooperation under IPEF.
- The United States should use IPEF to launch a partnership on government access to data—which is a foundational concern that underpins a wide array of restrictions on data flows, digital trade, and data governance in IPEF countries.
    - Progress on this issue is central to differentiating the United States and its likeminded democratic, rule-of-law countries from digital authoritarian countries like China and Russia who see physical access to data centers as a critical enabler of surveillance and political control.
    - The Department of Justice already has the mandate and expertise to work with the Department of Commerce on this issue.
    - The United States should also use IPEF to pursue updated MLATs, which would address a legitimate concern that governments have about data governance.
    - This will be difficult with India and Vietnam (and potentially Indonesia), but it's still worth including the issue, taking a fresh look at what is possible, and pushing those countries as far as possible.
- The United States should use IPEF to develop joint data sharing frameworks, which could include private firms, researchers, and organizations in specific sectors, such as health.

- The United States could even make participation in joint data sharing frameworks contingent on signing onto ambitious digital rules or at least demonstrating a genuine, good faith commitment to exploring alternative approaches to data localization, etc.

Innovation, Industrial, Economic, and Advanced Manufacturing Ideas for IPEF

- The United States could launch an IPEF innovation policy experts' group.
  - Each IPEF member country could nominate 3-4 people to work on a broad and/or specific set of innovation issues set by IPEF leaders. The expert group could meet periodically in working toward producing a report for IPEF leaders.
- The United States could work with IPEF partners to develop common industrial classification standards so that partners can conduct cooperative economic statistics gathering and more accurately assess supply chains.
- The United States could explore cooperation on Open Radio Access Network, or ORAN, equipment.
- United States should use IPEF to align collaborative international development aid/assistance, development finance support, and export credit initiatives to encourage nations in the Indo-Pacific region to select digital technologies, solutions, and platforms from vendors from like-minded nations.
- The United States should make joint supply chain mapping the foundation of efforts to improve supply chain resilience as it helps identify and address gaps.
- The United States should use IPEF to connect centers of excellence and advanced manufacturing firms with their international counterparts to share best practices and to build trade connections.
- IPEF could provide a platform for small to medium-sized enterprise (SME) manufacturers in participant countries with online access to digital manufacturing toolsets.

Use IPEF to Launch an Indo-Pacific Standards Strategy

- The United States should use IPEF to launch an "Indo-Pacific Standards Strategy" that would better connect standards-making bodies and related government agencies (and relevant industry stakeholders) on the development and use of standards (and certifications) for data, cybersecurity, AI, cloud services, and other new and emerging technologies.
  - If the United States doesn't mobilize the Department of Commerce, NIST, ANSI, and other agencies involved in technology standards, it essentially leaves a vacuum for China and the European Union, who are ramping up advocacy for a state-directed, restrictive, and discriminatory approach to standards setting that will inevitably disadvantage and discriminate against U.S. firms and products.
  - NIST and ANSI have not prioritized international standards cooperation and advocacy to the level it should—and it shows.

    - IPEF provides a chance for the United States to reset, catch up, and get ahead.
    - The United States should set up a high-level policy forum among the IPEF governments' standards experts (with an appropriate balanced scope of work given the government's interests and role in standards) on their respective approaches to new and emerging technologies and how best to address associated public policy issues, especially as it relates to the development and application of measurement standards.
        - Industry should be involved given their central role in developing and adopting technical standards as part of the open, transparent, and voluntary standard setting forums that the U.S. government supports.
        - A challenge to more forcefully advocating for the U.S.'s preferred approach to addressing certain tech and digital issues (e.g. NIST's Cybersecurity Framework and AI Risk Management Framework) is that these frameworks are voluntary, while the government plays a far more central, and prescriptive, role in many potential IPEF partner countries.
- IPEF should pursue pre-standardization cooperation on new and emerging technologies with IPEF partners.
    - This represents a creative, forward-looking way for the United States to work with likeminded partners on the early alignment of key terminology and concepts, technical details, and policy discussions, such as on AI, the Internet-of-Things, and facial recognition.
- The United States should use IPEF to advocate for the use of certifications (for services like cloud services) given they address legitimate public policy concerns (like cybersecurity) without unnecessarily impacting digital trade.
    - This is an important and indirect way to address concerns that some countries have about the security of U.S. cloud service providers (which they use to justify data localization).
- The Department of Commerce needs to work with its partner agencies (especially USAID and State) to better align and expand the resources and staffing dedicated to international standards policy engagement and to prioritize those countries that join IPEF.

Ideas for an IPEF Climate Change Agenda

- The United States should pursue an Indo-Pacific extension of its idea for a "climate club." The United States could extend what it is already doing with the EU in terms of a "green" steel deal or it could initiate a similar initiative but in another sector.
- The United States should use IPEF to coordinate clean energy supply chains.
    - The United States could build on recent steps in this direction, including those by the U.S. International Development Finance Corporation and the Department of Energy.

- The United States should use IPEF to create a regional climate change metrology center (run by NIST) to better measure, and therefore better understand and respond to, climate change.
    - NIST already has good relationships with counterparts in Australia, Korea, and Japan. With the proper funding, direction, and support, it could expand this network to other IPEF countries.
    - The United States could get NIST to work with counterparts to share information and best (methodological) practices and develop joint pilot projects to better measure climate change and associated activities and events.

Use IPEF to Launch a Joint Commercial Intelligence Forum

- The United States should launch a joint commercial intelligence forum at IPEF.
    - This would bring together respective agencies to share information, cases, and best practices when identifying and responding to foreign adversaries that seek to steal technology and trade secrets. The forum would focus specifically on combatting state-sponsored economic espionage in advanced-technology industries.
    - This would include enhanced information-sharing to combat foreign economic espionage and IP/technology/trade secret theft, including the use (and reform of) export control, foreign investment review, and other defensive mechanisms.
    - It would also include sharing information and best practices about how to ensure universities screen applications so that they do not educate people with direct connections to foreign (adversarial) governments (like China) in advanced technologies areas that have national security implications.

GLOBAL DATA FLOWS, PRIVACY, AND GOVERNANCE

The United States Trade Representative (USTR) leads IPEF's work on new digital trade rules, but the Department of Commerce has the responsibility and clear interests in key elements, especially as it relates to data. The United States **should use IPEF to make a few points explicitly clear on digital and technology governance, notably that European Union (EU) style harmonization is not the way to govern data and digital technologies in the global economy, but rather accountability and interoperability.**

One of the goals of IPEF should be to work to minimize the differences in digital regulation to better enable cross-border trade and investment. **The United States should leverage IPEF to reject the perspective (mainly European) that harmonization is the best approach to address global data, digital, and technology issues.** The EU's most direct means of conversion and coercion involves "adequacy" determinations. It negotiates with other countries about changes they will need to make to their privacy regimes so they can be deemed compliant with the terms of Europe's General Data Protection Regulation (GDPR) and thus worthy of managing EU personal data. To be sure, Europe has a right to regulate as it sees fit, as long as the standards apply equally to EU and non-EU firms doing business there. But it does not have a right to impose its standards on the rest of the world and then penalize nations that don't meet its standards.

Indeed, there is no reason why nations should not have different regulatory regimes for digital issues, as long as they are not de facto trade barriers and are broadly aligned to address key, common issues. Regulations don't need to be carbon copies to have a broadly similar effect. In other words, countries already regulate technologies differently. There is no reason why digital technologies should be any different. For example, there is nothing special about facial recognition technologies that suggests governance should be elevated beyond the national level (or EU level). Some places may ban it or impose heavy restrictions. Others may encourage its use, but with appropriate guidelines and protections. Those decisions should be up to the nations wherein the facial recognition is deployed. And to be clear this is not about avoiding a regulatory "race to the bottom." Quite the opposite. All nations should have regulations, but they should be based on a risk-based approach grounded in the innovation principle, not a harms-based approach grounded in the precautionary principle. As such, this is not a race to the bottom, but rather a race to the best: the best regulatory systems. It's up the United States to improve its game in developing and advocating for an alternative approach to digital and technology governance as part of IPEF.

When it comes to areas of regulation that involve cross-border impacts, the United States and its IPEF partners should work together to ensure their respective approaches are based on the principles of accountability and interoperability.

For example, **the United States should explicitly reference and articulate the principle of accountability in regards to data governance**—that privacy and other legal responsibilities move with the data. Rather than tell firms where they can store or process data, policymakers should hold firms accountable for managing data they collect, regardless of where they store or process it. Policymakers should focus on ensuring IPEF agreements, and their domestic legal frameworks, make clear that firms with a legal nexus in their jurisdiction are responsible for managing data in a certain way, wherever the data is transferred and stored.

Policymakers need to focus on an accountability-based approach rather than mistakenly believing that forcing firms to exclusively store data locally (a concept known as "data localization") is the only way to enforce data-handling requirements on foreign organizations. While any country can demand extraterritorial application of its laws, it may not always be able to enforce them (as this can be quite complex). Multiple criteria are used by courts to determine when a country has the authority to impose its laws on those outside of its borders. As long as a firm has a legal nexus within a country's jurisdiction, it has to abide by the laws of that country, regardless of where the firm stores data. Just as international financial firms operating in a foreign country fall under the purview of that country's local regulatory agencies, regardless of where they transfer money to, so do firms that collect and use data as part of their business within that region.

The United States should explicitly reference and articulate the principle of interoperability in regards to data governance. Interoperable privacy frameworks are the international extension of this accountability-based approach such that data is still able to flow between different privacy regimes, and countries' data protection rules flow with it. Modern technology, especially the Internet and cloud data storage, means that each country's domestic regulatory regime for data (such as for privacy) needs to be globally interoperable given that each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions. The goal for interoperability also reflects the fact that there will be no one globally harmonized privacy regime (as much as the European Union is trying to achieve harmonization through adequacy determinations). It is no surprise that interoperability—not harmonization or even adequacy—is a key objective of several of the leading data-protection initiatives, such as those of the Organization for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC). The United States should explicitly reference APEC's Cross-Border Privacy Regime in any data-related provisions and outcomes in IPEF.

An interoperable system would focus on "global protections through local accountability." The principle idea is that a country can enforce its rules on any foreign or domestic organization with legal nexus. Moreover, a country can enforce its rules on these organizations based on how they handle the data they collect, even if that data handling occurs abroad or with a third party. It is only through rigorous local enforcement that they are able to protect data globally. And it is this local enforcement that avoids the need to demand that all other countries abide by the same set of rules or pursue data localization policies.

The U.S. Congress is still contemplating enacting a comprehensive data privacy law. But this shouldn't preclude strong U.S. engagement on the issue in IPEF (as it's well assumed that whatever law the United States does potentially enact will be non-discriminatory). The United States is hardly alone in enacting or reforming data privacy and other key data-related laws, hence why IPEF should be based on interoperability between different systems that are built around common, core principles and processes.

The Chile-New Zealand-Singapore Digital Economy Agreement (DEPA) provides a useful model and set of provisions for IPEF to account for this fact in that **parties should create multiple different legal mechanisms to protect privacy of data transferred overseas**. Article 6 of DEPA module 4 on "Data Issues" states:

> "6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall pursue the development of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal information. These mechanisms may include: (a) the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement; (b) broader international frameworks; (c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or (d) other avenues of transfer of personal information between the Parties."[1]

Creating Conditionality: Align U.S. Development Assistance With Digital Trade and Strategic Interests and Allocate Greater Financial Resources (and Make Access Conditional) on Data and Digital Issues

The Department of Commerce, and its partners in other agencies, **need to better align U.S. development assistance with the commercial, trade, and strategic goals central to IPEF's digital and technology objectives and make access to ongoing and new digital development programs contingent upon genuine, good faith engagement in IPEF**.

Digital protectionists should not be able to benefit from U.S. Agency for International Development (USAID), U.S. Trade and Development Agency, Millennium Challenge Corporation, State Department, and other development-related funding. Likewise, the Department of Commerce should create conditional linkages within and between the various IPEF buckets. Access to new and useful funding and technical capacity assistance on certain digital issues is contingent on good faith engagement on associated cybersecurity or other digital issues that have been problematic.

How to Deal with India, Indonesia, and Vietnam and their Problematic Data and Digital Policies

The United States should obviously pursue ambitious trade law provisions that protect data flows and digital trade. However, the **United States should use a flexible approach, with connected contingencies, perhaps over an extended period of time (with the various workstreams moving at different speeds) to encourage those members with problematic policies to move toward these ambitious provisions**.

A central challenge for IPEF to make progress on supporting the free flow of data and digital trade will be to not simply replicate existing agreements (the benchmarks being the U.S.-Japan Digital Trade Agreement, digital economy agreements, and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership). **To add value to existing agreements, it is key that IPEF move Indonesia, India, and Vietnam closer to the U.S. approach to data and digital trade** (and that of Australia, Japan, New Zealand, and Singapore).

Motivations for problematic data policies in these countries vary, from digital protectionism, national security, and cybersecurity, to concerns about access to data, and surveillance.[2] The challenge is that direct confrontation by the U.S. government may not always be the best approach. Similar to what the United States did while it was part of the Transpacific Partnership (such as working with Japan on pharma-related interests), the United States should be tactical in working with select members that are likeminded on a specific issue and coordinate engagement with/by them. And to be creative in designing

For example, Vietnam's ongoing consideration of data localization as part of cybersecurity and content moderation laws is difficult to address. Vietnam knows the USTR's perspective. However, Singapore, which is central to ASEAN's work on data governance issues and is highly sophisticated in its approach to cybersecurity and other data issues, may be more relevant and effective in engaging with Vietnam to bring them along with the IPEF agenda and the U.S. goals for rules around data and digital trade. In the same vein, Singapore has adopted many parts of NIST's Cybersecurity Framework, so could use this as the basis for engagement with their Vietnamese counterparts as it relates to concerns about the security of government systems and data.

Similarly, the United States could create engagement by the U.S. Cybersecurity and Infrastructure Security Agency, the U.S. National Institute for Standards and Technology (NIST, detailed below), and others with Indonesia (and others) to share information and best practices about how to enact rules and regulations that protect government data and services (a legitimate issue that is, at least in part, motivating their consideration of data localization).

For example, in an ideal outcome, India, Indonesia, and Vietnam could become provisional partners of the digital trade law work led by USTR as long as they are genuinely, constructively engaged in the associated digital/tech module on cybersecurity and data protection technical capacity building, standards making, and

sharing of information and best practices. This will at least reveal whether the problematic proposals in these countries are genuinely (predominately, in the instance there are multiple motivations) motivated by concerns about cybersecurity and government access to data (and whether they're open to revising their approach) or simply by protectionism and surveillance. At a minimum, it would hopefully (at the bare minimum) convince them to narrow and minimize the extent of problematic data localization and other digital restrictions.

An additional idea is to **get IPEF/CPTPP members (such as Japan) to threaten to bring a CPTPP-based dispute case against Vietnam's use of data localization if it fails to join IPEF and engage in genuine, good faith cooperation**. As ITIF have argued, Vietnam's use of data localization in its Cybersecurity Law is likely a clear breach of the CPTPP's data-related provisions.[3]

In parallel, the United States should obviously work with building out the club of similarly ambitious countries on digital issues such as to create the corresponding incentive for these potentially problematic partners to join. Ultimately, by putting all the components together—the rules, the regulatory cooperation, the technical capacity building and information sharing, the supply chain cooperation and engagement, and the standards cooperation—the United States can create enough bucket-specific and overall incentives for these countries to reconsider and revise their problematic digital policies.

Developing New Domestic Laws and Trade Agreements and International Cooperation are Not Mutually Exclusive: They Can Happen in Parallel

Usually, international cooperation and trade rules follow well after each country's domestic debate around new laws and regulations pertaining to new and emerging technologies. **New digital trade rules are definitely needed** to prohibit and roll-back the growing range of barriers, **but these are insufficient on their own to future-proof (as much as possible) trade frameworks so that firms can engage in seamless cross-border digital trade and innovation**.[4] The pace of innovation and competition for every possible advantage in the global battle for tech leadership means U.S. trade policy also needs to be dynamic. **If the United States wants to create a truly free and open innovation- and digital trade-friendly framework, U.S. policymakers must build cooperation with likeminded trading partners to ensure the early and ongoing alignment in how they govern data and new digital technologies.**

Cooperation at the early stage of discussions around data and digital issues can hopefully lead to the sharing of information about how to best address them, while also avoiding policies that act as barriers to digital trade and data-driven innovation. This could cover data privacy, digital identity, payments, artificial intelligence (AI) governance, or some other issue. Such international cooperation shouldn't be left as an afterthought for years after a policy comes into effect. Unfortunately, this is China and the European Union's approach to

privacy, data flows, cybersecurity, and AI, which means they become country- and region-specific barriers to digital trade.[5] It's much harder to retrospectively change or work around these regulatory differences.

Australia, Chile, New Zealand, and Singapore are using digital economy agreements and memorandum of understanding (MOUs) to ensure the regulation of digital trade enablers like data innovation, AI, data portability, e-payments, e-invoicing, e-certification, trade facilitation, data privacy, the Internet of Things, blockchain, smart cities, and digital identity issues are aligned.[6] It allows the various partners to build a better understanding about respective approaches to new issues and to provide confidence and clarity around current arrangements and a connection between regulators as rules and technology change. The end goal is to ensure their respective approaches are interoperable—thus ensuring firms are able to work as seamlessly as possible across borders when conducting digital trade.

These **digital economy agreements show how truly modern trade agreements are as much about pursuing a model for digital governance that is international and interoperable as it is about agreeing on new, binding trade law provisions**.[7] It reflects a holistic approach in addressing both existing barriers while also working together to prevent new ones emerging as part of changing domestic laws and regulations. As Ravi Menon, Managing Director, Monetary Authority of Singapore (MAS), has stated, in the digital economy of the future data connectivity agreements among countries will become as important as today's free trade agreements.[8]

Revamp Regulatory Cooperation Between Agencies Involved in Data/Digital Issues

Revised and revitalized regulatory cooperation on digital issues would build greater trust and confidence between partner countries. U.S. agencies involved in privacy, financial oversight, and other digital-related issues may already have MOUs or international forums for cooperation, but due to a variety of reasons—such as a lack of capacity and resources, concerns that trade officials are infringing on their regulatory sovereignty, and the general perception that they're domestic, not international, agencies—they haven't updated, prioritized, or pursued closer engagement and cooperation with foreign counterparts.

For example, Singapore is leading the way in how its central bank (the Monetary Authority of Singapore, MAS) is pursuing agency-to-agency fintech MOUs with key counterparts in Australia, the United Kingdom, and the United States in order to support cross-border data flows, innovation, and digital trade in the sector. At the heart of these MOUs lies the recognition that however fintech evolves, the free flow of data and regulatory access to it will remain critically important to good governance, trade, and innovation (and that these goals are not mutually exclusive). The U.S. Department of Treasury is already heading in the right direction in agreeing to a MOU with MAS and flagging its interest in the issue more broadly.[9]

Regulatory cooperation around MOUs would ensure respective agencies share information at the earliest stages of the rulemaking process. It would also hopefully give other countries' governments and firms a seat at the table or ability to contribute feedback. Ultimately, it'd hopefully allow regulators to discuss issues, options, and ways to identify and eliminate differences in regulations—all in the shared interest of facilitating effective policy, and also trade and innovation.

Cooperation on enforcement—such as on shared privacy, cybersecurity, and financial oversight issues—should be part of greater regulatory cooperation. For example, the United Kingdom has taken steps in the right direction here. For example, on March 5, 2020, the UK's Information Commissioner's Office (ICO) and Australia's Information Commissioner signed an MOU to share information and best practices and to cooperate on specific projects and investigations. Following this, on July 9, Australian and British privacy regulators opened a joint probe into Clearview AI in order to examine how the company's facial recognition technology uses peoples' data.[10] Similarly, the ICO already has an MOU with New Zealand (on spam emails), the U.S. Federal Trade Commission, and Canada's Office of the Privacy Commissioner.[11]

A specific objective for IPEF would be for the United States and partners to review existing regulatory cooperation MOUs to ensure they cover the full spectrum of issues and provide a productive mechanism for information sharing, cooperation, and joint enforcement. Building better connections between enforcement agencies builds trust and confidence in domestic regulatory agencies that digital trade agreements and cooperation can help, not hinder, their ability to do their jobs.

Data Governance and Government Access to Data: Addressing the Root Cause of Many Digital Barriers (and Distrust in Data Flows to Some Countries)

The United States should **use IPEF to launch a partnership on government access to data—which is a foundational concern that underpins a wide array of restrictions on data flows, digital trade, and data governance in IPEF countries and between them and other trading partners.** Establishing transparent, balanced frameworks around government access to data is perhaps the most important thing the United States and its IPEF partners could do to build genuine trust as part of former-Japanese Prime Minister Abe's proposal for "data free flow with trust."

Progress on this issue is central to differentiating the United States and its likeminded democratic, rule-of-law countries from digital authoritarian countries like China and Russia, who see physical access to data centers as a critical enabler of surveillance and political control. Data localization enables political oppression by bringing information under government control and allowing the government to identify and threaten individuals, thereby impacting privacy, data protection, and freedom of expression.[12] China retains broad and vague legal authority in its laws to potentially access data for national security, public interest, and

political purposes.[13] The lack of an independent judiciary and the opaque nature of these laws make it hard to judge how China uses these broad powers.[14] Yet, this doesn't stop these countries from referring to "data privacy" as a motivation for localization.[15]

The United States has the institutional expertise and interagency partnerships to do this. The Department of Commerce's long history of work on this and associated issues related to data governance needs to expand, as does that by the relevant team at the Department of Justice (given its work on U.S. government access to data, Privacy Shield negotiations, engagement on CLOUD Act executive agreements, and Mutual Legal Assistance Treaties (MLATs)). Adding government access to data to IPEF would build on the valuable work both departments have been involved in on developing new principles on government access to data at the G7 and OECD. However, the United States should not wait until this G7/OECD work is completed to expand its engagement on the issue as time is of the essence (as more countries use concerns over government access to data to enact restrictions on data flows and digital trade) and its an issue of shared concern among countries around the world (it's not just a U.S.-EU issue with the European Court of Justice's Schrems I and II decisions).

The United States and other supporters for free flows of data increasingly hear the refrain from India (and others, such as Vietnam) about why they should allow the movement of data to China (a legitimate concern) as part of new rules and frameworks that support the free flow of data and digital trade. The United States obviously doesn't want to create barriers to data flows as part of IPEF, but if successful, discussions on government access to data could eventually be used to create (a positive) conditional data flow framework between the United States and IPEF partners that implement whatever agreement comes out of the G7/OECD process or they themselves develop. That data flows between these countries would be considered "trusted" as they involve countries that are all committed to international best practices as it relates to government access to data.

Australia, Japan, Korea, Malaysia, and New Zealand (and potentially Singapore, but it may be reluctant) would be the most likely countries to support IPEF work on government access to data. This would be a difficult issue to include in IPEF for both India and Vietnam, although India may be more "gettable." India is currently drafting a comprehensive data protection bill that includes localization and a broad carve out for government agencies (thus protecting its ability to access data).[16] Vietnam has long been weighing up localization measures as part of its Cybersecurity Law and more recently as part of online content laws and regulations. Its motivations for localization are often broad and vague: to protect national security, social order and safety, social ethics, and the health of the community.[17] Concerns about how Vietnam could use this to facilitate government access to data are real given the country does not have a dedicated, independent data protection agency; the responsible agency is the Ministry of Public Security.[18]

Use IPEF to Pursue Updated MLATs to Support "Data Free Flow with Trust"

The United States **should also use IPEF to pursue updated MLATs, which would address a legitimate concern that governments have about data governance** (in terms of law enforcement's ability to request and receive data related to criminal investigations). For example, electronic evidence is needed in around 85 percent of EU criminal investigations.[19] The problem is the current legal framework for managing law enforcement's cross-border requests for data is out of date and far too slow. New agreements and cooperation would improve law enforcement investigations while accounting for privacy and other concerns. It would provide Internet service providers with a clear legal framework to manage requests, and remove a motivation that some policymakers elsewhere around the world have used to try to justify data localization (in terms of facing issues with working through existing legal frameworks to access data stored overseas).

The Department of Justice already has the institutional experience and legal mandate to do this (such as via the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)). The United States has already enacted a CLOUD Act agreement with Australia. However, revising and expanding this work would require relevant U.S. agencies to change how they manage the issue. The Department of Justice (quite fairly) realizes that the prospects for a CLOUD Act executive agreement, with India for example, is out of reach for the meantime so backs off from engagement even though other efforts may help lay the groundwork for future progress (such as improving how their Indian counterparts prepare MLAT requests). Likewise, the Department of Justice often points to data-related restrictions as a trade issue for USTR to address (which obviously does not have the responsibility for addressing law enforcement-related concerns). The Department of Commerce often also engages on the issue in India and elsewhere, but it can only push so far given the Department of Justice's central role. But again, the Departments of Commerce and Justice have the institutional experience and relationships to do more, it just needs the strategic leadership and resources to expand their work on the issue to IPEF.

Support Open Data and Create Joint IPEF Data Sharing and Data Trust Frameworks

As the United States and its trading partners pursue national strategies to increase their competitiveness in AI, including via digital trade, it **should use IPEF to support the development of joint data trusts and other data-sharing models to improve the quality (and the quantity) of the data that is the key input into digital goods, services, and research.**

This matters because AI needs good data, not just more data.[20] For example, in a survey of 179 data scientists, over half identified addressing issues related to data quality as the biggest bottleneck in successful AI projects.[21] Therefore, it makes sense for the United States to use IPEF to encourage others to adopt open data frameworks for public data and data trusts and other models for the voluntary sharing of high-quality data.

"Open data" refers to data that is made freely available without restrictions.[22] Many governments have begun to embrace open data to encourage transparency and accountability, increase public participation, and promote economic growth. In many cases where high-quality data exists, it is dramatically underutilized. To this end, the United States itself is working through mechanisms to improve public-private data sharing.[23] The Open Data Inventory (ODIN)'s global index (of open data regimes for national statistical offices) ranked countries thusly for 2020-2021:[24]

- Singapore – 1st
- Korea and United States – tied for 22nd
- New Zealand – 25th
- Japan – 32nd
- Indonesia – 33rd
- Australia – 44th
- India – 64th
- Malaysia – 78th
- Vietnam – 91st

However, government data is only a fraction of the data that could be useful for AI development. For example, many major pharmaceutical companies have begun sharing historical clinical trial data with outside researchers, including competitors. Benefits include faster drug development, a better understanding of diseases, and more efficient clinical trials.[25] However, many stakeholders lack the mechanisms to share data while ensuring the protection of this proprietary and sensitive data. This highlights the government's role in identifying opportunities at home and abroad (with trade partners) to encourage the development and use of open data frameworks. If governments don't take on this coordinating role in identifying, developing, and supporting these data-sharing models, it is unlikely that organizations in many sectors will create them on their own.

To be clear, any data-sharing initiative should be voluntary and should not involve compulsory data divulsion. Only in cases where there is a clear market failure and firms control particular datasets for which they strictly limit access, should governments step in. Such a situation exists in the real estate and air travel industries in the United States.[26] Forcing companies to give up valuable data they have spent considerable time and money collecting and using to compete makes no more sense than forcing them to give up valuable patents, trade secrets, employees, or property.[27] It would undoubtably boost competitors, but it would also degrade a business's incentive to make future investments in these areas.

The United States should push for a specific open data section in IPEF, starting with the general recognition that opening up public information for re-use has considerable and widespread benefits to government, industry, and the public. The United States should require parties to have an open-by-default

framework for government data in place (without being prescriptive, as each country will approach the issue in their own way) and insist that trading partners should adhere to best practices for open data, including ensuring it is published in open, machine-readable formats. Given the need to avoid prescriptive frameworks, the United States should explicitly reference international agreements that signal that a country is committed to enacting best practices, such as the G8 Open Data Charter and the Open Government Declaration.[28]

The United States should propose MOUs and cooperative arrangements with partners to identify opportunities to build joint data-sharing frameworks between stakeholders in different countries and sectors. These datasets would be particularly useful for startup or other small organizations that do not have access to significant amounts of data. This could lead to sector-specific data trusts. For example, the Digital Catapult in the United Kingdom plans to publish model agreements for start-ups entering into data-sharing agreements.[29]

Use IPEF to Develop Joint Data Sharing Frameworks

The **United States should use IPEF to develop mutually beneficial data sharing frameworks, that could include private firms, researchers, and medical organizations in specific sectors—which may involve creating the technical architecture.** For example, the U.S. Department of Health and Human Services (HHS) recently announced proposed new rules that would facilitate access to patient data by both patients and the health care industry, in part by mandating the use of open application programming interface (APIs), which allow different software and databases to exchange data.[30] The United States could create similar models with IPEF countries. For example, IPEF health, data privacy, and other agencies could develop a data sharing framework to account for privacy, oversight, membership, and other issues so that interested partner countries and their firms could sign onto and contribute to sector-specific frameworks. For example, health firms could contribute data to a health data trust for members to use to support clinical trials on rare diseases or some other health issue. The **United States could even make participation in joint data sharing frameworks contingent on signing onto the ambitious digital rules or at least demonstrating a genuine, good faith commitment to exploring alternative approach to data localization etc.**

As part of this the United States may work with its partners to identify select circumstances where governments need to step in to encourage firms in particular areas to voluntarily share data. Although there is a net benefit from data sharing to patients and researchers, there is not always a short-term benefit to companies for making their data available to their competitors. A model effort is the Accelerating Medicines Partnership, a U.S. National Institutes of Health-led drug discovery collaboration among 10 drug makers, wherein participating companies have created a shared database that exceeds the capabilities of any individual company's data holdings.[31] Similarly, some pharmaceutical firms have recognized that sharing is in their collective interest and have participated in data-sharing programs, including the Accelerating Medicines Partnership and a GlaxoSmithKline-led initiative to share patient-level clinical trial data with other

participating pharmaceutical companies.[32] And the U.S. Health and Human Services Department recently announced proposed new rules that would facilitate access to patient data by both patients and the health care industry, by mandating the use of open APIs.[33]

INNOVATION, INDUSTRIAL, ECONOMIC, AND ADVANCED MANUFACTURING POLICY IDEAS FOR IPEF

There are several ideas the United States could pursue to support industrial development and economic cooperation among IPEF partners.

In addition to the specific ideas for supply chain resilience and advanced manufacturing cooperation (below), this could include:

- The United States could launch an IPEF innovation policy experts group (akin to the U.S.-China Innovation Policy Experts Group). Each IPEF member country could nominate 3-4 people to work on a broad and/or specific set of innovation issues set by IPEF leaders. The expert group could meet periodically in working towards producing a report for IPEF leaders.
- The United States could work with IPEF partners to develop common industrial classification standards—using North American Industry Classification System (NAICS) codes as the model—so that partners can conduct cooperative economic statistics gathering and collectively more accurately assess supply chains.
- The United States could work with IPEF on a joint productivity commission and studies so as to assess respective economic performance and understand how countries are working best to boost productivity.
- The wireless telecommunication industry is in the midst of a transition to more-openly defined protocols and interfaces in the radio portion of wireless networks, also known as Open Radio Access Network, or ORAN, equipment. This shift will lead to a more diverse, innovative, and secure wireless equipment market that is less likely to be dominated by companies supported by unfair Chinese practices. The United States could explore cooperation on ORAN equipment. The United States should encourage this transition by funding R&D and testbeds to identify challenges of manufacturing, integrating, and operating open radio equipment at scale.

Use IPEF to Better Align Export Credit Programs

The United States should work with IPEF partners to develop initiatives to address the changing global trade and economic landscape.

The elements to do so already exist. For instance, the Trump administration's Indo-Pacific strategy seeks to work with regional allies to advocate for free, fair, and reciprocal trade; open investment environments; good governance; and freedom of the seas.[34] Since an inaugural Indo-Pacific Business Forum in July 2018, U.S. government engagement has catalyzed private-sector investment in Indo-Pacific infrastructure, supported by

$2.9 billion through the Department of State and USAID, as well as hundreds of millions more through other agencies, including the U.S. Millennium Challenge Corporation (MCC) and the Overseas Private Investment Corporation (OPIC).[35] Meanwhile, the U.S. International Development Finance Corporation, created by the Better Utilization of Investments Leading to Development (BUILD) Act in 2018, will be providing $60 billion in development financing to attract more private-sector investment into global emerging markets.

The **United States should use IPEF to continue to work with these nations on collaborative international development aid/assistance, development finance support, and export credit initiatives to encourage nations in the Indo-Pacific region to select digital technologies, solutions, and platforms from vendors from like-minded nations**. A promising start is OPIC's launch of the Blue Dot Network, a multi-stakeholder initiative coalescing like-minded governments, the private sector, and civil society under shared standards of global infrastructure development.[36] But while programs such as Ex-Im's "Strengthening American Competitiveness Initiative" represent a step in the right direction, they could potentially be more impactful if they worked in lockstep with initiatives from like-minded countries, especially if developing nations in the region are considering significant national-scale digital infrastructure implementations—such as of 5G networks, smart-city implementations, or smart-grid networks—where collaborative bids from teams of enterprises from like-minded nations could be supported by common development finance or export credit assistance from their respective governments.

Supply Chain Resilience: Mapping to Identify and Address Gaps

The United States should **make joint (with Australia, Korea, Japan, and others) supply chain mapping the foundation of efforts to improve resilience as it helps identify and address gaps**.

For example, the U.S. Defense Production Act enabled the "Operation Warp Speed" ("OWS," a partnership between the Departments of Health and Human Services and Defense (DOD) to help accelerate the development of COVID vaccines) to intervene into supply chains, but key to that was an in depth understanding of every facet of relevant supply chains. DOD, under General Perna, was used to supplying U.S. troops in Middle East wars, had a strong emergency logistics capability, and knew the importance of supply chain reliability and flexibility and how to map them. It sprang into action, helping the companies with these supply issues and working to manage the application of the DPA to get key supplies to vaccine makers while not disrupting other needed markets. This supply chain mapping, and corresponding efforts to fill in gaps, was vital to OWS.[37] This mapping is already proving central to the effort to secure domestic supply chains for critical technologies and materials, and will be required in semiconductors, and for the technologies called for in the U.S. Innovation and Competition Act/COMPETES Act.

Advanced Manufacturing Cooperation

Nations are fiercely competing for manufacturing leadership, including through the development and use of high-performance computing (HPC) systems and other digital tools. Countries are developing national manufacturing digitalization strategies to support the broader development and use of these technologies.[38] However, if they wish to give their firms the best possible support, **the United States should use IPEF to connect centers of excellence and advanced manufacturing firms with their international counterparts to share best practices and to build trade connections.**

ITIF's report "Why Manufacturing Digitalization Matters and How Countries Are Supporting It" explains how digitalization is transforming manufacturing globally, detailing what exactly smart manufacturing is and examining the productivity impacts that digitalized manufacturing promises to deliver.[39] Whether it's called "Industry 4.0," as in Europe, the "Industrial Internet of Things (IIoT)," as in the United States, or simply "smart manufacturing," the application of information and communication technology (ICT) to every facet of manufacturing is in the midst of reshaping modern manufacturing, and thus, trade in manufactured goods.[40] Smart manufacturing is being driven by the advent and maturation of many technologies, including: HPC-powered computer-aided design (CAD) and engineering (CAE) software; cloud computing; the Internet of Things; advanced sensor technologies; 3D printing; industrial robotics; data analytics; machine learning; and wireless connectivity that better enables machine-to-machine (M2M) communications.

The United States could explore how to use IPEF to deepen linkages between America's Manufacturing USA network, Australia's Entrepreneurs Program, Japan's Industrial Value Chains Initiative (IVI), and other manufacturing-specific initiatives in other partner countries. Manufacturing USA consists of 16 manufacturing innovation institutes representing public-private partnerships. They focus on developing advanced manufacturing product and process technologies, facilitating their commercialization, and developing workforce skills around advanced manufacturing technologies.[41] Manufacturing USA plays a pivotal role in revitalizing the U.S.'s industrial competitiveness and ensuring U.S. leadership across a range of advanced-manufacturing processes and technologies.[42]

At least four Institutes of Manufacturing Innovation (IMIs) within Manufacturing USA address smart manufacturing-related technologies and processes. The first IMI, America Makes: The National Additive Manufacturing Innovation Institute, launched in 2011, focuses on expanding manufacturers' additive manufacturing (i.e., 3D printing) capabilities. The Digital Manufacturing and Design Innovation Institute (since renamed MxD) encourages factories across America to deploy digital manufacturing and design technologies, so America's factories can become more efficient and cost competitive.[43] The Institute for Advanced Composites Manufacturing Innovation (IACMI) accelerates the development and adoption of cutting-edge manufacturing technologies for low-cost, energy-efficient manufacturing of advanced polymer

composites for vehicles, wind turbines, and compressed gas storage.[44] Finally, the Clean Energy Smart Manufacturing Innovation Institute (CESMII) focuses on innovations such as smart sensors, data analytics, and controls in manufacturing that can dramatically reduce energy expenses in advanced manufacturing.[45]

The United Stated could use cooperation on defense-related research as a model to replicate for advanced manufacturing and the use of emerging technologies such as HPC. For example, on defense science and technology, the Five Eyes Technical Cooperation Program already involves many collaborative research and information exchanges, including on new and emerging technologies such as autonomy, the electromagnetic spectrum, advanced manufacturing, and urban environments.[46] In 2017, the United States added the United Kingdom (and Australia), to the National Technology and Industrial Base (a legal framework previously limited to the United States and Canada) to create new opportunities for joint R&D and controlled technology transfers.[47] Early "Pathfinder" projects are already underway exploring how this will open new avenues for cooperation involving the United States, Canada, Australia, and the United Kingdom.[48]

There are other non-defense models of cooperation to replicate. In September 2017, the United Kingdom and the United States signed the first-ever Science and Technology Agreement, which commits both nations to strengthening collaboration on research, science, and innovation.[49] The agreement sets out core agreements on the treatment of intellectual property, the confidentiality of data, and export controls.[50] It does not specifically mention advanced manufacturing or high-performance computing. However, in 2018, the U.S. Lawrence Livermore National Laboratory (LLNL) and the UK's governing body for scientific research signed a new three-year agreement to improve U.S. and UK industries through better use of high-performance computing, research collaboration, and joint economic promotion.[51]

Cooperation and engagement between the United States and its trade partners on HPC and advanced manufacturing won't lead to new binding rules. Instead, it'll build the framework to connect relevant policymakers and private-sector representatives to discuss, develop, and share best practices and connect firms that may be interested in working together on trade and research opportunities. It may take the form of government-to-government, agency-to-agency, or public/private MOUs that outline shared interests, principles, and best endeavors to consistently and proactively work together on shared public policy issues and in facilitating private-sector connections. This project could eventually evolve into formal exchanges and secondments between respective programs. However, it will take a concerted, considered effort for the United States to replicate this type of cooperation for key emerging manufacturing technologies with similarly ambitious and interested trading partners, whether it comes to Australia, Japan, India, Korea, Malaysia, or elsewhere. It's also a matter of identifying which trading partners prioritize the same technologies and where there are gaps in existing forums and agreements.

IPEF could help connect SME manufacturers in IPEF countries with online access to digital manufacturing toolsets.

IPEF could provide a platform for small to medium-sized enterprise (SME) manufacturers in participant countries with online access to digital manufacturing toolsets. For instance, America's MXD has created a facility called the Digital Manufacturing Commons (DMC) as a free, open-source software project to develop a collaboration and engineering platform that will serve as an online gateway for digital manufacturing.[52] Akin to an "app store for manufacturing," the DMC provides SMEs access to a digital services marketplace, including software development kits, essentially equipping SME manufacturers with high-performance computing empowered Computer-Aided Design (CAD), Computer-Aided Engineering (CAE), and other advanced modeling and simulation tools they need to address technical design challenges.[53] In most cases, SMEs would be unable to afford either the needed sophisticated IT hardware or software, so this approach democratizes access to advanced computing and computational systems for SME manufacturers. IPEF could set up a similar instrument to benefit SME manufacturers.

USE IPEF TO LAUNCH AN INDO-PACIFIC STANDARDS STRATEGY

The United States should use IPEF to launch an "Indo-Pacific Standards Strategy" that would better connect standards making bodies and related government agencies (and relevant industry experts) on the development and use of standards (and certifications) for data, cybersecurity, AI, cloud services, and other new and emerging technologies. The United States should ensure there is a major standards component in IPEF in order to develop a legitimate alternative for partners in IPEF (and elsewhere) to consider and adopt as they all try to find the best way to address legitimate issues raised by data and new and emerging technologies. **If the United States doesn't mobilize the Department of Commerce, NIST, ANSI, and other agencies (and relevant industry stakeholders) involved in technology standards, it essentially leaves a vacuum for China and the EU, who are ramping up their own efforts to advocate for a state-directed, restrictive, and discriminatory approach to standards setting that will inevitably disadvantage and discriminate against U.S. firms and products.**

The United States should use IPEF to:

- **Launch an "Indo-Pacific Standards Strategy."**
- **Set up a high-level policy forum among the IPEF governments' standards experts (with an appropriate balanced scope given the government's interests and role in standards)** on their respective approaches to new and emerging technologies and how best to address associated public policy issues, especially as it relates to the development and application of measurement standards.
- **Setup cybersecurity, cloud services, AI, and critical infrastructure security modules to exchange information and best practices, such as NIST's Cybersecurity Framework.**

- Many U.S. digital policymakers fail to appreciate the significance of NIST's Cybersecurity Framework, in terms of how it has become a global, adaptable model (in comparison to the EU and China's respective (restrictive) approaches).
- Industry should definitely be involved given their central role in developing and adopting technical standards as part of the open, transparent, and voluntary standard setting forums that the U.S. government supports.
    - This highlights a key challenge for the United States advocating for NIST's Cybersecurity Framework and AI Risk Management Framework and related work is that many parts of it are voluntary. It does not involve the government as a central actor with prescriptive and legally binding laws, which is the case in many countries in the Asia-Pacific. Even given this, NIST's Cybersecurity Framework stands out as a ready-made reference point for a cybersecurity sub-module. Statements from policymakers around the world show its use and value.[54] Singapore has adopted much of NIST's Cybersecurity Framework.
- It would be significant if NIST was able to do the same for AI and other new and emerging areas, with IPEF countries adopting or adapting NIST's cybersecurity and AI frameworks and the U.S. Federal Risk and Authorization Management Program (FedRAMP). Progress on these issues would (hopefully) indirectly address related (legitimate) motivations (such as on national security and cybersecurity) that some policymakers in the region misuse as motivation for data localization and other restrictive policies (such as in India, Indonesia, and Vietnam). Again, industry should have a clear role to play given their expertise and role in developing new standards.

- To **pursue pre-standardization cooperation on new and emerging technologies, such as AI and facial recognition (detailed below).** Thus, even if countries take different legal approaches to regulating new and emerging technologies, firms have the advantage of basing their technology on the same foundational, technical elements (in terms of terminology, measurement methodology, and other technical processes) as other leading tech-driven trading partners, such as Australia, Japan, and the United States. All of this can be done well before standards are finalized and part of regulatory systems that are much harder to change once enacted.
- To **advocate for the use of certifications (for services like cloud services) given they address legitimate public policy concerns (like cybersecurity) without unnecessarily impacting digital trade (detailed below).**

Standards define some specific characteristic or function for a specific item (which may be, for instance, a material, a product, a procedure, a process, or a service), to make such an item meet certain well-defined objectives (which may relate, for instance, to performance or interoperability).[55] Standards can be physical,

reference material, a measurement protocol, documentary standard, a technical specification, a guidance document, or a best practice. Standards development work is a collaborative activity that engages a wide array of subject matter experts from the private and public sectors including industry, government, academia, and standards development organizations (SDOs).[56]

Standards play an important role in the global race for innovation and trade advantage in new and emerging technologies, whether it's 5G, AI, data privacy, facial recognition, advanced manufacturing, digital finance, or other sectors. Given their role, there are two faces to the standards coin: cooperation and collaboration vs. competition. However, with similarly ambitious, tech-focused, and value-sharing partners, the former can be important for firms from both parties to help them compete, especially against firms from other countries or regions that use restrictive standards.

Divergent standards are often an obstacle to spreading technologies and hamper interconnection and interoperability. Even worse, they can impede the development and deployment of new technologies if stakeholders don't coalesce around one widely agreed upon approach. For example, it may lead to reduced or hedged investments across new and emerging technologies as tech firms (and investors) wait and see which standard prevails. Standards unique to a country (such as China) or region (such as the European Union) make it more difficult and costlier for foreign firms and their products to be sold in those markets as they need to reconfigure preexisting design and production processes to suit those specific standards, and pay royalty fees for providing products using the local standard. This disrupts the global, generally standardized production processes on which many foreign companies rely. It leads to fragmentation in standards, resulting in increased costs for consumers while simultaneously reducing choices.

China provides a clear example of how country-specific standards can act as a barrier to trade for high-tech goods and services.[57] As ITIF's report "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" argues, China has made the development of indigenous technology standards, particularly for ICT products, a core component of its industrial development strategy.[58] Similarly, Richard Suttmeier's "A New Technonationalism?: China and the Development of Technical Standards" details the early 2000s battle over China's efforts to promote its own wireless communications standard WAPI (wireless authentication and privacy infrastructure), which continues to have many technical issues and has never been adopted widely, even in China.[59] Most recently, in 2018, China introduced a new standardization law that will likely favor local firms and goods and services, as it references "indigenous innovation" while failing to reference either its WTO commitments (therefore raising questions about WTO compliance) or its acceptance of existing international standards (as approved by the various SDOs).[60]

The United States is paying more attention to (technical) standards setting processes and organizations (like the International Telecommunications Union (ITU)). It has the U.S. Standards Strategy (last updated in

2020), but it isn't nearly as prominent or strategic as what other countries have done. It does not have the formal, comprehensive standards strategy like the EU's recently announced Standardization Strategy or China's National Standardization Development Outline (known as "China Standards 2035").[61] China is actively pushing Korea and Japan, and their respective firms, to use their approach to standards. Meanwhile, the EU's strategy explicitly seeks to not only have the government play a central role in standards development, but to export its approach and to provide development assistance to do this.[62] While the United States should not emulate the EU and China's state-centered approach to standards (as the U.S.'s approach is based on open, voluntary, and industry-driven approach to developing technical standards), it's clear the United States needs to up its game on technology governance advocacy and engagement, especially in the Asia Pacific, to develop an alternative to these state-directed, restrictive approaches to standards setting that are not aligned with U.S. commercial and strategic interests.

The Department of Commerce, NIST, and the American National Standards Institute (ANSI) all have a major potential role to play. NIST's role should be central here. **NIST should play a far more proactive role in engaging with counterparts on the development and adoption of (technical) standards that reflect U.S. values and interests.** NIST has (incidentally) developed and demonstrated some of the policy capabilities that the United States should (massively) expand upon in creating a much larger role for NIST in U.S. engagement on digital, technology, and climate change engagement around the world, including at IPEF. NIST needs to develop real policy capabilities as part of a renewed mission around international engagement and development of standards.

NIST does valuable work that has a major impact on the United States and globally (such as the broader adoption of NIST's cybersecurity framework). NIST is central to U.S. government engagement on the development and adoption of (technical) standards. NIST is held in high regard. Its credibility comes from its commitment to an open and data-driven approach to standards discussions. It is not seen as political (as standards bodies in other countries are seen).

But to be frank, given what's at stake and America's leading role in technology, NIST has not prioritized international standards cooperation and advocacy (e.g. at the ITU and at the bilateral and regional levels) to the level it should—and it shows. The same could be said for ANSI, which has a paltry international development program.[63] NIST has not engaged near as much as it should have. NIST's engagement on standardization issues has varied greatly, and given significant staffing changes, this has led to extended periods of time with no engagement at standards development organizations. **The few dedicated U.S. government staff at NIST and other agencies that work on technical standards discussions are stretched thin. They also often struggle to get attention, resources, and support from their superiors, who do not themselves understand the international standards work and its relevance. Often times managers (at NIST and other agencies) view standards engagement as a cost with benefits that do not**

manifest immediately. As standards engagement often requires international travel, many agencies have extremely bureaucratic processes to approve such travel and engagement (e.g. requests having to be submitted more than 6 months in advance of the meeting). In specific regards to the ITU, at times, NIST senior and mid-level leaders have not prioritized it as they don't understand the ITU and the standardization activities there. All this needs to change. Furthermore, the coordination that the United States needs to achieve with likeminded partners on new and emerging technologies only grows in importance. IPEF could be an opportunity for the United States to upgrade its approach to federal government standards cooperation and alignment/interoperability with key partners on a range of critical issues and technologies.

Australia, Japan, Korea, Malaysia, New Zealand, and Singapore would likely support IPEF work on standards. India may not support it as they have sometimes enacted discriminatory local standards as part of an effort to disadvantage U.S. tech firms and products and are potentially attracted to China's strategic use of discriminatory standards (for this same reason, to disadvantage foreign firms and products).

Expand NIST (and ANSI's) Resources and Role in International Standards Engagement and Capacity Building

The **Department of Commerce needs to work with its partner agencies (especially USAID and State) to better align and expand the resources and staffing dedicated to international standards policy engagement and to prioritize those countries that join IPEF.**

ANSI and NIST have limited dedicated resources and initiatives for international capacity building (see examples below). And USAID doesn't have to design and implement programs that contribute to trade and strategic policy goals. It's unclear what new funding and policy support is involved in the U.S. Digital Connectivity and Cybersecurity Partnership (led by the USAID and the Department of State), but it does not appear substantive.[64] NIST used to have a much larger dedicated support program called "Standards in Trade."[65] However, a NIST manager nixed the long-standing program despite its many successes. Currently, NIST provides minimal technical input to ANSI and USAID-funded programs being implemented by ANSI. There is a great need, and certainly a huge opportunity, for NIST to step up to the plate—in partnership with the Department of Commerce, ANSI, and others.

The United States is in a race with China and the EU to influence how countries and regions around the world regulate digital policy issues and design and use standards. As mentioned, the EU uses development assistance to advocate for its approach to standards. The EU and its member states already provide considerable assistance to many countries on digital issue, including embedding officials to work specifically on standards policy. The United States has tried to take some steps in the right direction in allocating more,

new funding to digital economy policy issues in developing countries (such as the USAID's Digital Strategy), but more needs to be done and quicker. For example, in an effort to take a leaf from the EU's playbook and embed a person in the African Union's unit working on the digital extension of African Continental Free Trade Area, it took USAID, USTR, and others more than three years to place someone.

Pre-Standardization Policy Cooperation on New and Emerging Technologies

Pre-standardization cooperation is a creative, forward-looking way for the United States to work with likeminded partners on the early alignment of key terminology and concepts, technical details, and policy discussions. There are existing forums and cases to show the value of pre-standardization cooperation on new and emerging technologies.

For example, in 1982, regulatory agencies and laboratories from G8 countries (now the G7) and the EU came together as part of the Versailles Project on Advanced Materials and Standards (VAMAS) to develop standardized terminology, reference materials, and testing and measurement protocols for new materials (physical, chemical, material, electronics etc.).[66] As part of the inter-laboratory testing (also referred to as round robin testing) processes, VAMAS stakeholders sent samples to multiple labs to test draft protocols they'd developed to see if the results from different participating laboratories got the same results and to identify where the protocol didn't work and how to correct it. VAMAS stakeholders had an MOU with the International Organization for Standardization (ISO) to help feed their pre-standardization cooperation into the formal standards-making process.[67] This MOU has greatly benefited both organizations, as is evident by the strong cooperation between VAMAS Technical Working Areas addressing nanotechnology-related measurements and the ISO Technical Committee 229 (Nanotechnologies), which is chaired and supported by BSI. VAMAS continues to work on a range of physical materials, with an expanded membership, including Brazil, Mexico, South Africa, Australia, India, and China.[68] Its work was (and remains) useful as it allows the final, consensus standards to be based on the same terminology and measurement and testing procedures.

Other examples of pre-standardization work involve researchers from Germany, Japan, and the United States working together on electrokinetic measurements and quantification of coarse particle content (such as those used in advanced materials, thermal coatings, and drug carriers).[69] Another example involves standards-related collaboration between NIST and the European Commission's Joint Research Center (ECJRC) for the development of reference materials for nanotechnology and health-related measurement standards.[70] Another recent example involves nanomaterials and measuring toxicity at the nanoscale.[71]

Pre-standardization cooperation is a technical and scientific, not political, process. Given standards are a key part of the battle for innovation advantage between the United States, China, the EU, and others, it can be

much harder to cooperate and coordinate on standards for more mature technologies as the technologies are built out and they become increasingly tied to political objectives, built up infrastructure, sunk investment costs, and enacted (and thus hard to change) laws and regulations. For firms and other stakeholders, pre-standardization work can be easier than final-stage formal standards development as they're not already heavily invested in existing standards guidance. Trying to change standards for mature technologies can be problematic given the cost and complexity involved in ensuring future and backward compatibility (i.e., retooling design and production processes to suit a new standard). This is why pre-standardization cooperation could be a more pragmatic objective for standards cooperation as it is technically focused and done at the early stages of technological innovation, before potential uses and outcomes have been politicized or broadly adopted and deployed by firms.

For firms and other stakeholders engaged in cutting-edge research, such early-stage cooperation gives them an opportunity to inform discussions, learn from peers, and help inform potential standards and policy objectives. Pre-standardization cooperation also accelerates the formal standards development process. Standards that are informed by these pre-standardization efforts would obviously benefit participants given it'd align with their products and processes.

The **United States should work with IPEF partners and their stakeholders (those involved in technology standards, whether from government, academia, or the private sector) to identify opportunities for closer, more active cooperation on pre-standardization discussions for new and emerging technologies.** A first step would be for the United States to map existing agreements, fora, and coordination mechanisms and identify gaps and areas for pre-standardization cooperation. It'd ensure their respective stakeholders are engaged with likeminded partners at the earliest stages of technological innovation in discussing and working toward common foundational elements for potential future standards. It could involve identifying use cases for the technology at the heart of the standards process and associated ethical, societal, and governance concerns.

The United States has already implemented part of the foundation for a more-targeted, active approach to pre-standardization cooperation on new and emerging technologies. In particular, the Trump Administration's Executive Order on Maintaining American Leadership in Artificial Intelligence tasks NIST with developing a plan for federal engagement in the development of technical standards (including international standards) and related tools in support of reliable, robust, and trustworthy systems that use AI technologies.[72] NIST has released a plan for the development of standards for artificial intelligence, including the goal to work with likeminded countries on development of AI standards and related tools.[73] Together, this framework and strategy provides a platform for NIST and other U.S. agencies to potentially work with their IPEF counterparts to identify shared priorities in standards for new and emerging technology.

NIST has already done a range of work that could form the basis for a broader agenda to work with IPEF partners on digital and data-related pre-standardization discussions. NIST has led efforts to develop globally accepted standards, guidelines, and practices and to advocate for its Framework for Improving Critical Infrastructure Cybersecurity—seen by many as the global standard of best practices for cybersecurity.[74] Since its publication in 2014, the Framework has been updated, translated into various languages, and adapted by government and industries across the globe.[75] NIST has had an active engagement strategy.[76] The UK has introduced several corresponding pieces of law which mirror the framework, including its minimum cybersecurity standard and networks and information security directive.[77] This is indicative of the potential for greater UK-U.S. collaboration and cooperation.

But NIST's work on this should be expanded to other areas, including Internet-of-Things (IoT) systems and devices, next generation communication technologies, and data-related issues. The development of AI standards—particularly technical standards—is at a very early stage in both countries and elsewhere around the world. For example, most national AI strategies refer to the development of standards for ethical and trustworthy AI. But technical standards to support this goal are still in the early stages of development. The United States is trying to fill this gap. It'd be beneficial to IPEF if government agencies and firms would be involved to ensure they are able to inform and align their technology with the U.S.'s approach, given it'll shape a large part of the global market. Likewise, U.S. stakeholders would benefit by feeding into IPEF partners' thinking around standards and regulation.

For example, **the United States could collaborate with IPEF partners on establishing a framework to characterize and measure the trustworthiness of AI systems.** For example, terms like "algorithmic transparency" and "algorithmic bias" do not yet have a technical definition.[78] Moreover, the United States and partners could collaborate on building and using common datasets to develop and test measurement and testing protocols. These programs would provide AI developers in the United States and IPEF partners with useful guidelines for designing and testing AI systems, allow for the comparison of AI systems, and inform future legislation and regulatory actions.[79] The United States could also work with NIST and others to develop shared, representative datasets of faces to serve as a more reliable resource for organizations developing facial recognition technology.[80] It could involve best practices for producing explanations or justifications of decisions made by AI systems.[81] NIST is working on both these issues (including via workshops) in a domestic context.[82]

Cloud Service Security Auditing and Certification

The United States **should include a separate IPEF sub-module or topic (perhaps under cybersecurity or how to better protect critical infrastructure) to work on cloud service auditing and certifications.** Data localization and other restrictions on data and U.S. firms and products, especially cloud providers, are

sometimes due to a misunderstanding about what actually goes into good cybersecurity, but also in part, due to a general distrust of U.S. cloud providers (as clearly evident in India, Indonesia, and Vietnam).

U.S. cloud providers are thoroughly audited and use industry-based certifications to demonstrate their commitment to protecting their customer's data. The United States, meaning agencies such as those involved in FedRAMP, could include work on best practices in terms of regulations, auditing, and certifications as a way to show what good cybersecurity actually looks like (and indirectly as a way of showing the security of U.S. cloud providers). FedRAMP (governed by the Department of Defense, the Department of Homeland Security, and the General Services Administration) is designed for providers working with federal agencies (which is a key area of concern for Indonesia, Vietnam, India, and others as it relates to cloud services), it also involves NIST guidelines (Special Publication 800-53) which can be used as a framework for any industry, given its broad scope of security controls.[83]

IDEAS FOR AN IPEF CLIMATE CHANGE AGENDA

The United States should pursue an Indo-Pacific extension of its idea for a "climate club." As ITIF argues, levying carbon tariffs is a difficult and counterproductive way for nations with ambitious climate policies to create a level playing field for their higher-cost industrial sectors. A more workable solution would be to design a flexible open-trade club for climate innovators.[84] The United States could extend what it is already doing with the EU in terms of a "green" steel deal or it could initiate a similar initiative but in another sector. The goals of a climate innovation club include sustaining international trade, encouraging the flow of innovative technologies across borders, driving increasingly ambitious climate targets, and spurring investment in hard-to-abate sectors, all while building upon the Paris Agreement's bottom-up approach, which respects national sovereignty and allows for policy flexibility.[85]

The United States should use IPEF to coordinate clean energy supply chains. The United States could build on recent steps in this direction. For example, the U.S. International Development Finance Corporation funded a solar panel plant in India (being built by First Solar, an American firm).[86] The U.S. Department of Energy's recent report on "America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition" provides some useful ideas, including:

- Ensure that implementation of the U.S. government clean technology competitiveness export strategy harnesses the clean technology demand pull of international markets in a way that supports domestic manufacturing.
- Explore establishing multilateral coordination mechanisms on voluntary energy transition-related critical material stockpiling, including through the International Energy Agency.
- Establish and fund an initiative for expanding clean technology manufacturing capacity globally to achieve the dramatic scale-up in manufacturing of key climate and clean energy equipment associated with meeting net-zero commitments.[87]

Get NIST to Help IPEF Partners Better Measure Climate Change as a Way to Help Them Better Understand and Prepare for It

The **United States should use IPEF to create a regional climate change metrology center to better measure, and therefore better understand and respond to, climate change.**

Without much fanfare or attention and with minimal resources, since 2012, NIST has been developing tools to better measure various climate change components and related activity.[88] Metrology—the science of measurement, embracing both experimental and theoretical determinations at any level of uncertainty in a field of science and technology—is central to NIST's work. At the moment, global efforts to better address climate suffer from the fact that measurement tends to be at the micro level (e.g., sensors on the ground next to an industry smoke stack) or at the macro level (e.g., hugely expensive satellites that collect data). This leaves a gulf in terms of data for policymakers to better understand the production and spread of chemicals that contribute to climate change and the impact of adverse climate change-related events at the town or community level and how this differs across countries. For countries to deploy larger climate change-related budgets or cap-and-trade, or carbon tax mechanisms, they need better data. Current measurements do not provide a high degree of confidence.

NIST already has good relationships with its counterpart organizations (the national measurement institutions) in Australia, Korea, and Japan. With the proper funding, direction, and support, it could expand this network to other IPEF countries. The United States could get NIST to work with counterparts to share information and best (methodological) practices and develop joint pilot projects to better measure the components that contribute to climate change and associated activities and events. One country's approach to measurement may be specific to its country or to a specific a community, so IPEF would be valuable as it would potentially include a diverse set of countries that are each facing different types of climate change challenges, whether it's bushfires in Australia or coastline erosion in Indonesia. This type of cross-country testing of measurement methodologies by different agencies and laboratories is normal at NIST and in the world of measurement standards (known as "round robin testing" or inter-laboratory comparisons). Thus, its potential cross-country application could be attractive to a broad range of countries.

NIST is already involved in some initiatives that resemble the type of activity that it would need to greatly expand with this initiative under IPEF. For example, NIST does this in measurement related issues with countries in the Americas through the SIM regional grouping. There's also the Asia Pacific Metrology Program (APMP), which NIST could contribute to as part of an expansion (its participation would also be greatly welcome). For example, in past years, the APMP Focus Group on Metrology for Climate Change involved Korea, Japan, Singapore, and India. Its objectives were:

- To establish to the national climate measurement standards related to climate change;
- To exchange information on how to support the national body of climate change by national measurement institutes (so that it is measurable, reportable, and verifiable);
- To give strategic advice to national measurement institutes on climate change programs.[89]

USE IPEF TO LAUNCH A JOINT COMMERCIAL INTELLIGENCE FORUM

The United States **should use IPEF to launch a joint commercial intelligence forum** to bring together respective agencies to share information, cases, and best practices when identifying and responding to foreign adversaries that seek to steal technology and trade secrets. The forum would focus specifically on combatting state-sponsored economic espionage in advanced-technology industries. In many ways, it would resemble a commercial equivalent of the defense-focused Five Eyes (intelligence sharing) Alliance to address predatory, nonmarket-driven Chinese trade and economic activity. Many potential IPEF members have updated their laws and regulations, and pursued certain cases, in recent years that highlight potential areas for greater cooperation and policy alignment.

A joint commercial intelligence forum could include:

- Developing a comprehensive list of enterprises and individuals who have attempted or effected IP theft, and develop mechanisms to restrict such firms and individuals from competing in like-minded nations' markets.
- Enhanced information-sharing efforts to combat foreign economic espionage and IP/technology/trade secret theft, including their use (and reform of) respective export control, foreign investment review, and other defensive mechanisms. In many ways, it'd be similar to the U.S.-EU Trade and Technology Council's cooperation on export controls and foreign investment reviews.
- Sharing information about best practices to ensure universities screen applications so that they do not educate people with direct connections to foreign (adversarial) governments (like China) in advanced technologies areas that have national security implications. For example, since 2007, China's People Liberation Army has sponsored more than 2,500 military scientists and engineers to study abroad and has developed relationships with researchers and institutions across the globe. This collaboration is highest in "Five Eyes" countries, Germany, and Singapore.[90]

The United States could use the IPEF commercial intelligence cooperation to develop a more ambitious and effective plurilateral approach to promulgate export controls, foreign investment screening, and other defensive measures. IPEF partners could develop such a plurilateral regime for semiconductors specifically, or for a broader set of advanced technologies (e.g., AI, 5G, quantum, etc.) along with semiconductors. IPEF countries could work together to establish a common understanding of both what threats are posed to specific

advance technology sectors by enterprises from non-market economies not fundamentally competing on market-based terms.

RECIPROCAL, MUTUALLY BENEFICIAL COOPERATION ON SCIENTIFIC RESEARCH

The **United States should create a new scientific engagement platform within IPEF, with a specific focus on other parts of the IPEF agenda (such as digital governance, climate change etc.).**

IPEF scientific cooperation should be based on the principle of reciprocity. The U.S. government (like others) has engaged in extensive cooperation with China to help share valuable technology in areas such as energy, health, and agriculture.[91] Yet the expectation from the Chinese side is this should happen regardless of China's ongoing innovation mercantilism and discriminatory approach to foreign technology and trade. For example, the U.S.-China Clean Energy Research Center's Technology Management Plans state participants shall negotiate in good faith to provide nonexclusive licenses for IP developed on joint projects with participants in the other country, as well as with third parties that are not participants. Yet, "[a]ccording to agency officials, this has not been the case in previous science and technology agreements between the United States and other countries."[92]

IPEF parties should discuss how they can work together with their respective universities to advance scientific progress and foster cooperation, while ensuring any research collaboration is in their national interests and not supporting Chinese military research efforts. As much as IPEF parties should not be helping China's self-interested pursuit of innovation mercantilism, they should also not be helping rivals leverage open, good-faith academic research programs in order to develop their own military expertise and technology. Both are clearly not in their respective national interests, yet it remains unclear whether Western universities and governments are fully aware of this phenomenon.[93] Parties should talk about the issue and policy guidance for universities. Given the technologies involved, this issue should also be discussed in the context of cooperation on improved export control regimes.

ENDNOTES

1 "Digital Economy Partnership Agreement "DEPA" Between Singapore, Chile, and New Zealand," https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Chile-New-Zealand-Singapore-21-Jan-2020-for-release.pdf.

2 Nigel Cory, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

3 Nigel Cory, "Vietnam's cybersecurity law threatens free trade," *Nikkei Asian Review,* August 15, 2018, https://asia.nikkei.com/Opinion/Vietnam-s-cybersecurity-law-threatens-free-trade.

4 Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"; Nigel Cory, "Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade" (The Information Technology and Innovation Foundation, June 30, 2020), https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff; Nigel Cory, "Response to the Public Consultation for the European Commission's White Paper on a European Approach to Artificial Intelligence" (The Information Technology and Innovation Foundation, June 12, 2020), https://itif.org/publications/2020/06/12/response-public-consultation-european-commissions-white-paper-european.

5 Eline Chivot and Nigel Cory, "Response to European Commission Consultation on Transfers of Personal Data to Third Countries and Cooperation Between Data Protection Authorities" (The Information Technology and Innovation Foundation, April 29, 2020), https://itif.org/publications/2020/04/29/response-european-commission-consultation-transfers-personal-data-third; Cory, "Response to the Public Consultation for the European Commission's White Paper on a European Approach to Artificial Intelligence."

6 For example, "Australia-Singapore Digital Economy Agreement: summary of key outcomes," Australia's Department of Foreign Affairs and Trade, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-summary-key-outcomes

7 "Australia-Singapore Digital Trade Standards," TRPC presentation, March, 2020, https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-trade-standards-presentation.pdf.

8 Ravi Menon, "Singapore FinTech: Innovation, Inclusion, Inspiration: speech," November 12, 2018, https://www.mas.gov.sg/news/speeches/2018/singapore-fintech.

9 In 2018, MAS and the U.S. Commodity Futures Trading Commission (CFTC) signed a similar MOU: https://www.cftc.gov/sites/default/files/2018-09/cftc-mas-cooparrgt091318_16.pdf; U.S. Department of the Treasury Under Secretary McIntosh stated: "Data connectivity facilitates financial regulators' access to the financial risk-related data needed to fulfil their mandates in ensuring safety and soundness….When data connectivity is impeded, firms, consumers, regulators, and the economy as a whole are all worse off, and we risk losing out on many benefits of today's digital economy, https://home.treasury.gov/news/press-releases/sm900.

10 "The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.," UK's Information Commissioner's Office, July 9, 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

11 "ICO's blog on its international work," UK's Information Commissioner's Office, https://ico.org.uk/about-the-ico/news-and-events/icos-blog-on-its-international-work/; "FTC Signs Memorandum of Understanding with UK Privacy Enforcement Agency," U.S. Federal Trade Commission website, March 6, 2014, https://www.ftc.gov/news-events/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency; "MOU Between the Privacy Commissioner of Canada and the Information Commissioner of the United Kingdom," https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-memorandums-of-understanding/mou-uk/.

12 Erica Fraser, "Data Localisation and the Balkanisation of the Internet," SCRIPTed, 2016, Vol. 13, p. 359, https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/.

13 Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare blog post, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Samm Sacks, Qiheng Chen, and Graham Webster, "Five Important Takeaways From China's Draft Data Security Law," DigiChina Project blog post, July 9, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/.

14 Bill Bishop, "One country, one Internet?; TikTok; Gaokao; Floods in China; US FBI head on China," Sinocism newsletter, July 7, 2020, https://sinocism.com/p/one-country-one-internet-tiktok-gaokao.

15 For example, Russia stated that its personal data localization requirement (enacted in 2015) was to "provide extra protection for Russian citizens both from misuse of their personal data by foreign companies and surveillance of foreign governments." Alexander Savelyev, "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?" Computer Law & Security Review, 32 (2016) 128–145, https://doi.org/10.1016/j.clsr.2015.12.003; "Russia's security service tells internet firms to hand over user data: The Bell," Reuters, February 12, 2020, https://www.reuters.com/article/us-russia-internet/russias-security-service-tells-internet-firms-to-hand-over-user-data-the-bell-idUSKBN2060UV.

16 Adnan Ahmad Ansari, "India's Data Protection Bill–the long wait continues," The Atlantic Council, January 21, 2022, https://www.atlanticcouncil.org/blogs/southasiasource/indias-data-protection-bill-the-long-wait-continues/.

17 Thomas Treutler and Giang Thi Huong Tran, "Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees," Lexology, December 18, 2019, https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd.

18 For example, the director general of the Department of Cybersecurity and High-Tech Crime Prevention and Control under Vietnam's Ministry of Public Security is responsible for deciding on the required deletion, sending written requests for deletion to the relevant entities and auditing such entities' compliance with the LOC. "Updates to Draft Decree Detailing Certain Articles of Law on Cybersecurity," Baker McKenzie blog post, October 8, 2019, https://www.bakermckenzie.com/en/insight/publications/2019/10/updates-draft-decree-law-on-cybersecurity.

19 "Frequently Asked Questions: New EU rules to obtain electronic evidence," European Commission website, https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345.

20 Joshua New, "AI Needs Better Data, Not Just More Data," Center for Data Innovation blog, March 20, 2019, https://www.datainnovation.org/2019/03/ai-needs-better-data-not-just-more-data/.

21 "Data Scientist: 2017 Report" (CrowdFlower, industry report, 2017), https://visit.figure-eight.com/rs/416-ZBE-142/images/CrowdFlower_DataScienceReport.pdf.

22. Open Data Handbook, "What is Open Data?", Open Knowledge Foundation, 2012, http://opendatahandbook.org/en/what-is-open-data/.

23 Dave Nyczepir, "As data-sharing becomes more crucial, agencies say industry can help with privacy issues," *Fed Scoop,* July 8, 2020, https://www.fedscoop.com/data-privacy-government-cots-census-bureau/.

24 "Global Rankings 2020," Open Data Watch, https://odin.opendatawatch.com/Report/rankings.

25 "Project Data Sphere® Cancer Research Platform Achieves Key Milestones: Data from More 100,000 Patients and Over 133 Research Studies," Press Release, December 13, 2017, https://www.businesswire.com/news/home/20171213005674/en/Project-Data-Sphere%C2%AE-Cancer-Research-Platform-Achieves; Joshua New, "The Promise of Data-Driven Drug Development" (The Center for Data Innovation, September 18, 2019), https://www.datainnovation.org/2019/09/the-promise-of-data-driven-drug-development/.

26 Daniel Castro, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (The Center for Data Innovation, November 6, 2017), https://www.datainnovation.org/2017/11/blocked-why-some-companies-restrict-data-access-to-reduce-competition-and-how-open-apis-can-help/.

27 "Response to the European Commission's Consultation on the European Strategy for Data" (The Center for Data Innovation, 2020), http://www2.datainnovation.org/2020-eu-data-strategy.pdf.

28 "Open Government Declaration," https://www.opengovpartnership.org/process/joining-ogp/open-government-declaration/.

29 "Artificial intelligence, digital technology and advanced production" (Organisation for Economic Cooperation and Development, 2020), https://www.oecd-ilibrary.org/sites/629af843-en/index.html?itemId=/content/component/629af843-en.

30 "Notice of Proposed Rulemaking to Improve the Interoperability of Health Information," U.S. Department of Health and Human Services, https://www.healthit.gov/topic/laws-regulation-and-policy/notice-proposed-rulemaking-improve-interoperability-health.

31 Damian Garde, "Big Pharma superteam joins NIH to share data, discover new drugs," *FierceBiotech*, February 4, 2014, https://www.fiercebiotech.com/partnering/big-pharma-superteam-joins-nih-to-share-data-discover-new-drugs.

32 Harlan Krumholz, "Time To Assess Pharma Progress In Data Sharing," *Forbes*, June 2, 2014, https://www.forbes.com/sites/harlankrumholz/2014/06/02/time-to-assess-pharma-progress-in-data-sharing/.

33 "Notice of Proposed Rulemaking to Improve the Interoperability of Health Information."

34 United States Department of State, "A Free and Open Indo-Pacific: Advancing a Shared Vision" (2019), 2, https://www.state.gov/wp-content/uploads/2019/11/Free-and-Open-Indo-Pacific-4Nov2019.pdf.

35 Ibid.

36 U.S. Department of State, "A Free and Open Indo-Pacific: Advancing a Shared Vision," 16.

37 William Bonvillian, "Emerging Industrial Policy Approaches in the United States" (ITIF, October 4, 2021), https://itif.org/publications/2021/10/04/emerging-industrial-policy-approaches-united-states.

38 Stephen Ezell, "Why Manufacturing Digitalization Matters and How Countries Are Supporting It" (The Information Technology and Innovation Foundation, April, 2018), http://www2.itif.org/2018-manufacturing-digitalization.pdf.

39 Ibid.

40 Stephen J. Ezell, "A Policymaker's Guide to Smart Manufacturing," (Information Technology and Innovation Foundation, November 2016), 1, http://www2.itif.org/2016-policymakers-guide-smart-manufacturing.pdf.

41 Manufacturing USA, "How We Work," https://www.manufacturingusa.com/pages/how-we-work.

42 David M. Hart, Stephen J. Ezell, and Robert D. Atkinson, "Why America Needs a National Network for Manufacturing Innovation" (Information Technology and Innovation Foundation, December 11, 2012), https://itif.org/publications/2012/12/11/why-america-needs-national-network-manufacturing-innovation.

43 "The Institute," Digital Manufacturing and Design Innovation Institute, accessed October 4, 2016, http://dmdii.uilabs.org/the-institute/technology.

44 "About," The Institute for Advanced Composites Manufacturing Innovation, accessed October 30, 2016, http://iacmi.org/about-us/.

45 The White House, "FACT SHEET: President Obama Announces Winner of New Smart Manufacturing Innovation Institute and New Manufacturing Hub Competitions" news release, June 20, 2016, https://www.whitehouse.gov/the-press-office/2016/06/20/fact-sheet-president-obama-announces-winner-new-smart-manufacturing.

46 "Technical Cooperation Program," https://www.dst.defence.gov.au/partnership/technical-cooperation-program.

47 George Costa, "Five Eyes Ministers commit to advance defence and security cooperation," *International Insider,* June 24, 2020, https://internationalinsider.org/five-eyes-ministers-commit-to-advance-defence-and-security-cooperation/; "10 U.S. Code § 2500 – Definitions," https://www.law.cornell.edu/uscode/text/10/2500.

48 "Fiscal Year 2017: Annual Industrial Capabilities: Report to Congress," U.S. Department of Defense, April 12, 2018, https://www.businessdefense.gov/Portals/51/Documents/Resources/2017%20AIC%20RTC%2005-17-2018%20-%20Public%20Release.pdf?ver=2018-05-17-224631-340.

49 "The United States and United Kingdom Sign Landmark Science and Technology Agreement," The White House, September 20, 2017, https://www.whitehouse.gov/articles/united-states-united-kingdom-sign-landmark-science-technology-agreement/.

50 "UK/USA: Agreement on Scientific and Technological Cooperation [TS No.25/2017]," https://www.gov.uk/government/publications/ts-no252017-ukusa-agreement-on-scientific-and-technological-cooperation.

51 "LLNL/U.K. officials ink agreement to collaborate on HPC research, ensure competitiveness," February 14, 2018, https://www.llnl.gov/news/llnluk-officials-ink-agreement-collaborate-hpc-research-ensure-competitiveness.

52 James Barkley, Digital Manufacturing and Design Innovation Institute, phone interview by Stephen Ezell, ITIF, March 4, 2016.

53 Ibid.

54 "NIST Cybersecurity Framework: International Perspective," NIST website, https://www.nist.gov/cyberframework/international-perspectives.

55 United Nations Industrial Development Organization (UNIDO), *Role of Standards: A Guide for Small and Medium-Sized Enterprises* (Vienna: UNIDO, 2016), https://pnirajan.files.wordpress.com/2016/12/tcb_role_standards.pdf; "Understanding ICT Standardization: Principles and Practice," European Telecommunications Standards Institute, 2018, https://www.etsi.org/images/files/Education/Understanding_ICT_Standardization_LoResWeb_20190226.pdf.

56 For example, for additive manufacturing. "Standardization Roadmap for Additive Manufacturing," America Makes and ANSI, June, 2018, https://share.ansi.org/Shared%20Documents/Standards%20Activities/AMSC/AMSC_Roadmap_June_2018.pdf.

57 Office of the United States Trade Representative (USTR), "2018 National Trade Estimate Report on Foreign Trade Barriers" (Washington, D.C.: USTR, 2018), https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

58 Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (Information Technology and Innovation Foundation, December 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.

59 Richard P. Suttmeier, "A New Technonationalism?: China and the Development of Technical Standards," *Communications of the ACM,* Aril 2005, Vol 48, No 4, pages 35-37, https://cacm.acm.org/magazines/2005/4/6260-a-new-technonationalism/fulltext.

60 Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018," https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

61 European Commission, "New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market," press release, February 2, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661; Patrick Lozada, Tim Ruhling, and Helen Toner, "Chinese Involvement in International Technical Standards: A DigiChina Forum," DigiChina, December 6, 2021, https://digichina.stanford.edu/work/chinese-involvement-in-international-technical-standards-a-digichina-forum/.

62 European Commission, "An EU Strategy on Standardisation - Setting global standards in support of a resilient, green and digital EU single market," February 2, 2022, https://ec.europa.eu/docsroom/documents/48598.

63 "ANSI International Development Programs," ANSI, https://www.ansi.org/trade-development/development-programs/ansi-programs.

64 "The Digital Connectivity and Cybersecurity Partnership," USAID, https://www.usaid.gov/digital-development/digital-connectivity-cybersecurity-partnership.

65 "NIST's Standards Coordination Office: Standards in Trade Workshop Program," NIST, 2014, https://www.nist.gov/system/files/documents/2016/12/07/sco_onepager_sit_workshops_02262014.pdf.

66 "MOU between the Versailles Project on Advanced Materials and Standards (VAMAS) and the International Organization for Standardization (ISO), https://www.nims.go.jp/vamas/refarences/lndldd000000045h-att/MOU_VAMAS_ISO.pdf; "Versailles Project on Advanced Materials and Standards (VAMAS)," http://www.vamas.org/.

67 Ibid.

68 "Current active TWAs," http://www.vamas.org/twa/active.html.

69 "Ceramics Division: Materials Science and Engineering Laboratory: FY 2002 Programs and Accomplishments," U.S. National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6904.pdf.

70 "JRC and NIST explore further common areas of work in certified reference materials for nanotechnology and health-related measurement standards," European Commission website, March 27, 2014, https://ec.europa.eu/jrc/en/science-update/jrc-and-nist-explore-further-common-areas-work-certified-reference-materials-nanotechnology-and.

71 Gerard Riviere, "European and international standardisation progress in the field of engineered nanoparticles," *Inhal Toxicology*, Jul 21, 2009, Suppl 1:2-7, https://pubmed.ncbi.nlm.nih.gov/19558227/; Ajit Jillavenkatesa, "US-EU Workshop on Bridging nanoEHS Research Efforts," U.S. National Institute of Standards and Technology presentation, December 3, 2013, https://www.us-eu.org/wp-content/uploads/2013/12/Jilla-Slides.pdf.

72 "Executive Order on Maintaining American Leadership in Artificial Intelligence," White House, February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

73 "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools," U.S. National Institute of Standards and Technology, August 9, 2019, https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

74 "Framework for Improving Critical Infrastructure Cybersecurity," U.S. National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

75 "International Resources: Cybersecurity Framework," U.S. National Institute of Standards and Technology, https://www.nist.gov/cyberframework/international-resources

76 Amy Mahn, "Continuing to Strengthen International Connections on the Cybersecurity Framework," U.S. National Institute of Standards and Technology blog post, April 21, 2020, https://www.nist.gov/blogs/cybersecurity-insights/continuing-strengthen-international-connections-cybersecurity-framework.

77 "How does UK legislation match up to the NIST Cybersecurity Framework?," Quorum Cyber blog post, https://www.quorumcyber.com/blog/2018/11/21/how-does-uk-legislation-match-up-to-the-nist-cybersecurity-framework.

78 Alistair Nolan, *Artificial intelligence, digital technology and advanced production* (Paris: Organisation for Economic Cooperation and Development), https://www.oecd-ilibrary.org/sites/629af843-en/index.html?itemId=/content/component/629af843-en.

79 Michael McLaughlin, "The National Artificial Intelligence Initiative Act Could Strengthen U.S. AI Leadership" (Center for Data Innovation, March 21, 2020), https://www.datainnovation.org/2020/03/the-national-artificial-intelligence-initiative-act-could-strengthen-u-s-ai-leadership/.

80 "To Measure Bias in Data, NIST Initiates 'Fair Ranking' Research Effort," U.S. National Institute of Standards and Technology blog post, November 14, 2019, https://www.nist.gov/news-events/news/2019/11/measure-bias-data-nist-initiates-fair-ranking-research-effort.

81 "Draft White Paper on Combinatorial Methods for Explainability in AI and Machine Learning," U.S. National Institute of Standards and Technology, May 22, 2019, https://www.nist.gov/news-events/news/2019/05/draft-white-paper-combinatorial-methods-explainability-ai-and-machine.

82 "Exploring AI Trustworthiness: Workshop Series Kickoff Webinar," U.S. National Institute of Standards and Technology, August 6, 2020, https://www.nist.gov/news-events/events/2020/08/exploring-ai-trustworthiness-workshop-series-kickoff-webinar.

83 "How NIST 800-53 Maps to FedRAMP," Lightedge website, October 22, 2020, https://www.lightedge.com/blog/how-nist-800-53-maps-to-fedramp/#:~:text=While%20FedRAMP%20is%20designed%20for,manufacturing%20to%20the%20end%20user.

84 Stefan Koester, David Hart, and Grace Sly, "Unworkable Solution: Carbon Border Adjustment Mechanisms and Global Climate Innovation" (ITIF, September 20, 2021), https://itif.org/publications/2021/09/20/unworkable-solution-carbon-border-adjustment-mechanisms-and-global-climate.

85 Ibid.

86 "DFC Announces Approval to Provide up to $500 Million of Debt Financing for First Solar's Vertically-Integrated Thin Film Solar Manufacturing Facility in India," U.S. International Development Finance Corporation, press release, December 7, 2021, https://www.dfc.gov/media/press-releases/dfc-announces-approval-provide-500-million-debt-financing-first-solars.

87 U.S. Department of Energy, "America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition," February 24, 2022, https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition.

88 "NIST: Climate," https://www.nist.gov/climate.

89 "NIST APMP Focus Group: Metrology for Climate Change," NIST, https://www.nist.gov/document-18428.

90 Alex Joske, "Picking flowers, making honey" (Australian Strategic Policy Institute, October 30, 2018), https://www.aspi.org.au/report/picking-flowers-making-honey.

91 Richard P. Suttmeier, Trends in U.S.-China Science and Technology Cooperation: Collaborative Knowledge Production for the Twenty-First Century? (Washington, D.C.: U.S.-China Economic and Security Review Commission, September 11, 2014), https://www.uscc.gov/sites/default/files/Research/Trends%20in%20US-China%20Science%20and%20Technology%20Cooperation.pdf.

92 United States Government Accountability Office (GAO), "U.S.-China Cooperation: Bilateral Clean Energy Programs Show Some Results but Should Enhance Their Performance Monitoring" (Washington, D.C.: GAO, July 2016), 33–34, http://www.gao.gov/assets/680/678321.pdf.

93 Alex Joske, "The China Defence Universities Tracker," (The Australian Strategic Policy Institute, November 25, 2019, https://www.aspi.org.au/report/china-defence-universities-tracker.