Policy Memo for the Biden-Harris Administration and the 117th Congress:

Advancing Innovation to Make the U.S. More Globally Competitive

January 2021

ITI

Promoting Innovation Worldwide

The United States is a global leader in innovation and technology. The U.S. policy and regulatory environment has enabled American companies to lead the world in developing innovative products and services, including groundbreaking, disruptive technologies that transform markets, address societal challenges, and allow us to imagine entirely new solutions that facilitate creation and commercial engagement by an increasingly wide range of firms, entrepreneurs, and individuals.

This means that the United States enjoys significant benefits from policies that promote research and development (R&D), digital trade, and technological innovation – and those benefits reverberate through all sectors of the U.S. economy and society. This has become even more evident as the COVID-19 pandemic has highlighted the indispensable role that technology and the technology sector play in enabling hundreds of millions of Americans to work, learn, and connect with one another. However, the pandemic has helped expose racial inequities in access to digital skills and technology, which are necessary to participate in the economic opportunities of the digital economy, requiring action to address these inequities. Strengthening U.S. technological competitiveness and prioritizing diversity, equity and inclusion in our sector provides an unprecedented opportunity to ensure that the benefits of the United States' success are shared broadly throughout its economy.

The U.S. spends more on R&D than any other country, accounting for 25 percent of global expenditures, with the private sector funding a large majority of R&D investments and primarily driving the expansion in R&D spending. However, China is increasingly a close second, accounting for 23 percent of global spending on R&D. The discoveries realized through U.S. R&D investments fuel U.S. global competitiveness, both through the creation of high-paying jobs across the United States, as well as through developing and selling the products and services those innovations offer to global customers. The jobs and economic benefits flowing from these successes are present throughout the U.S. economy and society, with all sectors and geographies benefiting from technology and innovation-driven activity. For example, farmers can compare data sets over time to increase yields without accelerating degradation of the land, and manufacturers can precisely track production across their supply chains to ensure the highest levels of quality. We also see the benefits from increasing access to broadband internet service and internet-enabled technologies, facilitated by powerful and innovative computing capabilities, such as cloud computing, that allow innovators to build or expand IT-enabled enterprises anywhere they choose, whether in a sprawling metropolis, a small town, or a rural area. And as we make investments in the technologies necessary to achieve a low-carbon future we will realize new opportunities to create jobs and spur economic growth.

At the same time, breathtaking advances in the innovation and adoption of information and communications technology (ICT) have blurred the lines between local and global firms by

allowing new ways for firms to conduct business across borders. These changes call into question the notion of a separate, digital economy; the modern global economy depends implicitly on the responsible movement of digital information across borders. Globally competitive companies across all sectors rely on data, a vast array of computer and data-driven technologies, and a robust and resilient global supply chain to produce, export, market, and sell goods and services, evidenced by the fact that global cross-border data flows grew by 45 times from 2005 to 2015. By 2015, the global value of cross-border data flows had surpassed the value of trade in goods for the first time in history, with some 75 percent of that value accruing to companies outside the technology sector, primarily through gains in growth, productivity, and employment. Technology products and services increasingly drive growth and job creation in virtually every sector of the economy, whether extending opportunities for care through telehealth, innovating environmental solutions, customizing consumer experiences, optimizing manufacturing operations, building capacity to achieve a low-carbon future, or through new ideas and opportunities that continue to be developed.

The fact that every U.S. state has a stake in the success of the increasingly technology-driven economy increases the urgency for policymakers to act decisively to strengthen U.S. competitiveness. As other countries increase their investments and advance new approaches to digital policy, the U.S. faces the risk of falling behind and losing its global share if it fails to demonstrate a meaningful commitment to driving U.S. technological competitiveness. This risk has been amplified by the economic challenges that face the U.S. as it responds to and recovers from the global pandemic. Below we outline a range of policies that advance the goals of promoting U.S. economic competitiveness and securing the consequent benefits to the broader U.S. economy.

Contents

Tax Policy

Tax policy not only helps drive competitiveness, but is an effective tool to support economic growth, promote job creation, and encourage innovation. To realize these goals, policymakers should ensure that the U.S. maintains an internationally competitive tax system, including a competitive and fiscally responsible corporate tax rate. Policymakers also have the opportunity to leverage tax policy to promote growth in high-skilled, highly paid jobs, including by supporting innovation and technology manufacturing and ensuring that groundbreaking R&D activities and valuable intellectual property are located in the United States. Improving the competitiveness of U.S. tax policies helps enable the competitiveness of its economy as a whole.

ITI Recommendations

1 Policymakers should ensure that the tax code continues to incentivize investment in R&D in the United States.

We strongly support efforts to provide federal support for R&D, and one powerful way to do so is through the tax code. An immediate, critical step that policymakers should take is protecting the current treatment of R&D expenses for tax purposes. The U.S. currently ranks 26th out of 36 countries on the Organisation for Economic Co-operation and Development's (OECD) index that evaluates the competitiveness of R&D tax incentives. Despite this already poor showing, the U.S. is poised to drop further when the ability for companies to immediately deduct R&D expenses is eliminated starting in 2022. Policymakers should seek to reverse this trend by preserving the current treatment of R&D expenses and should look to identify other tax policy levers to promote R&D investment in the United States.

2 The Administration should prioritize multilateral engagement culminating in an agreement to ensure a cohesive global tax system and to counter the ongoing proliferation of unilateral digital services taxes.

Engaging globally with allies to reach a multilateral consensus at the OECD will increase certainty for businesses worldwide and turn the tide against the proliferation of unilateral tax measures that contravene key international tax policy norms and impact the competitiveness of U.S. companies in the global market. An agreement to ensure a cohesive global tax system will provide predictability to businesses, alleviate the fragmentation perpetuated by digital services taxes and other discriminatory unilateral tax measures, and enable companies to thrive globally. The Administration should continue to pursue strong engagement at the OECD and with the U.S. Congress to achieve these outcomes, while securing commitments from governments to withdraw any proposed or enacted digital services taxes that target U.S. companies.

Artificial Intelligence

Artificial Intelligence (AI) is a key technology that offers enormous societal benefits, including improvements on sustainability, public health and safety, and economic growth. Many countries around the world are working to harness the benefits of AI while also addressing challenges that may emerge. AI technology and policy are still evolving, and as such, the United States has a substantial opportunity to be a global leader in designing a smart, proportionate regulatory model, shaping voluntary standards, and determining how this technology is regulated. However, such leadership requires thoughtful, light-touch regulatory approaches and global partnerships. This will allow for continued AI innovation and growth, strengthening the competitiveness of U.S. companies, while also building trust in AI applications.

ITI Recommendations

1 Implement OMB memo M-21-6, Guidance for the Regulation of Artificial Intelligence Applications.

ITI appreciates the initial steps taken by the U.S. government in finalizing the OMB Memorandum, which emphasizes the importance of a foundation of public trust of AI. This approach will help to encourage innovation and bolster competitiveness by avoiding overly prescriptive regulatory treatment of AI applications, encouraging agencies to be thoughtful in how they address challenges that may arise in the use of particular AI applications, and allowing the U.S. government to adopt a holistic approach to governing the use of AI. We encourage U.S. policymakers and the new Administration to continue following this trajectory, by embracing the OMB Memorandum and EO 13859, ensuring that agencies submit the required plans.

2 The Administration should continue engagement with international partners and in multilateral fora to align global AI-related norms and guidance wherever possible.

Countries and international stakeholder organizations around the world have proposed a variety of norms and guidelines to govern AI and have, in some cases, launched regulatory efforts to address concerns about impacts of, and use cases for, AI. While we recognize there are some concerns related to bias in AI systems, a one-size-fits-all approach to regulating AI technology itself is not the answer. Instead, we recommend a thoughtful, measured approach to AI governance, which considers the level of risk associated with specific AI applications and use cases and is informed by international standards. As such, we urge the Administration to continue engaging in multilateral fora, such as the Global Partnership on Artificial Intelligence (GPAI) and the OECD, as well as bilaterally, to encourage risk-based approaches and reliance, wherever possible, on international norms and standards.

3 The Administration should seek to increase funding for AI R&D and continue to support the activities being undertaken by NIST on AI.

Increasing basic R&D funding, including through the National Science Foundation (NSF), National Institutes of Health (NIH), Department of Energy (DOE), and Department of Defense (DOD), will drive forward innovation in foundational technologies that will power AI. Allocating additional funding to agencies such as the National Institute of Standards and Technology (NIST), which is undertaking a host of activities on AI, including research on measuring and enhancing trustworthiness of AI systems and developing standard benchmarks and datasets, will also help to facilitate greater investment in and adoption of AI technology.

Cybersecurity & Supply Chain Security

The reliance of the global economy on digital products and services makes the confidentiality, integrity, and availability of those products and services fundamental to consumer trust, both domestically and with international partners. The federal government's ability to provide consistent regulatory approaches and supply chain security guidelines, while maintaining regular information sharing practices, are critical elements of providing the effective cybersecurity necessary to garner that trust. Securing the U.S. innovation economy and ensuring supply chain resiliency are shared responsibilities that will facilitate the global competitiveness not only of the U.S. technology sector, but of any segment of the economy reliant upon digital devices and the internet.

ITI Recommendations

1 Congress and the Administration should promote a thoughtful, harmonized, risk-based, evidence-driven approach to cyber and supply chain security policy.

This should include prioritizing increased funding for R&D and innovation, supply chain resiliency investments, government-wide IT modernization, and workforce development. Approaches that are non-design neutral, globally fragmented, or duplicative may hinder the ability of U.S. companies to innovate and compete globally on technology and security solutions. Facilitating U.S. competitiveness requires investment in security and technology modernization as well as in the resiliency of U.S. manufacturing. Measures should be informed by fundamental security policy principles such as design neutrality, facilitating interoperability and scalable harmonized approaches to security (leveraging international standards and avoiding state and federal fragmentation), supporting private-public partnerships, favoring evidence-driven, risk-based approaches to security, and avoiding duplicative or localized requirements (e.g. in the domain of security certification) that may stifle growth and innovation to address ever-evolving cyber threats.

2 The Administration should streamline and harmonize ongoing government efforts to improve cybersecurity and supply chain resilience.

One way to do this is by empowering the National Cyber Director within the White House and designating CISA as the lead agency to coordinate supply chain risk management efforts. Working together, the Cyber Director and the Cybersecurity and Infrastructure Security Agency (CISA) could ensure coordinated, coherent, and consistent policymaking across the federal government in these areas. At the same time, such a streamlined approach will ensure that the federal government is able to widely and effectively leverage modern cyber and supply chain technologies. The tech sector shares policymakers' concerns regarding threats to global ICT supply chains, which implicate not only cybersecurity but also national security and economic security. However, this concern has manifested in uncoordinated, inconsistent approaches across the interagency. We encourage the President to consider a nominee for National Cyber Director with the background and experience necessary to unite the intelligence and military equities with the capacity and authorities of the Homeland Security, Law Enforcement, and Commercial communities, to ensure more constructive engagement across the federal government. Additionally, establishing a lead agency on supply chain risk management will help establish a coordinated and effective approach to disparate activities at all levels of government.

3 U.S. policymakers should leverage the existing ICT Supply Chain Risk Management Task Force as a focal point for public-private collaboration on supply chain security.

Policymakers should work with leadership to develop a strategic plan to establish long term support for the Task Force as a venue to co-develop solutions with industry to the nation's most pressing supply chain security challenges. The Task Force has brought together subject matter experts from the private sector and from across the US government and has produced several actionable tools and other work products that can be used by industry and government to address supply chain security challenges, including related to information-sharing, threat modeling, procurement, and vendor attestation. Addressing supply chain security threats requires a holistic approach and the Administration should look first to this established public-private mechanism for creative, actionable solutions, and should prioritize implementing and operationalizing Task Force products across the U.S. government and incentivizing their promotion and uptake across the critical infrastructure community.

4 The Administration should focus the scope of EO 13873, ensuring that covered transactions are prioritized and targeted according to discrete national security risks.

In its current form, the EO and associated rulemaking will have potentially devastating effects on U.S. competitiveness and innovation, casting a cloud of uncertainty over almost all ICTS transactions with foreign entities, with limited benefit to ICTS security. We agree that supply chain security is imperative to facilitating trust, but the EO in its current state does not achieve those objectives, in large part because it focuses on risks associated with foreign adversaries to the exclusion of other risk-based considerations related to the ICTS supply chain. Therefore, revising the EO and/or its rulemaking scope to ensure it is targeted at identifying and managing the greatest risks would allow U.S. companies to conduct global business with certainty, thus improving competitiveness and allowing for continued innovation across borders.

Privacy

Privacy and user trust are central to our member companies' businesses and global operations. Consumer trust is a key pillar of innovation, and our industry must do everything it can to deepen that trust and meet our customers' expectations when it comes to protecting their privacy and personal data. Privacy policy and data protection measures are essential mechanisms to enable innovation while upholding the individual rights of citizens who entrust companies with their personal data.

ITI Recommendations

1 Congress and the Administration should advance a comprehensive federal privacy regime.

Such regime should codify strong privacy protections that enhance transparency, increase consumer control over personal data, promote security, and ensure continued innovation by providing a uniform approach to data protection regardless of where a consumer resides. The current landscape of privacy and data protection regimes around the globe and in the U.S. is increasingly complex and challenging to navigate,

undermining data innovation practices and negatively impacting consumer welfare. To counter these trends and offer policymakers an alternative approach to data protection, ITI released the Framework to Advance Interoperable Rules (FAIR) on Privacy principles in 2018. This data protection framework embraces consumers' and policymakers' desire for greater privacy protections by advancing individuals' data control rights and clearly defining the responsibilities of companies using personal data while also recognizing the importance of data to the innovations that transform people's lives and advance the public interest. Streamlining regulatory approaches in this manner is intended to offer the world a strong data protection approach that enhances trust and enables innovation to flourish while also creating efficiencies in compliance and enabling the better investment of resources in people and innovation.

2 Rapidly conclude an agreement with the European Commission in the wake of the Schrems II ruling, and more broadly, develop and reinforce mechanisms to facilitate cross-border transfer of data and ensure the privacy of citizens.

The free flow of data is fundamental to the U.S. economic recovery and national competitiveness. U.S. policymakers should rapidly conclude negotiations on an enhanced transatlantic data transfer agreement with the EU. Such an agreement is essential to ensure continuity of commercial activities involving data flows and should respect European citizens' fundamental rights as well as the legitimate security and public safety interests of governments around the world. More broadly, the USG should promote global cooperation and interoperability between regional mechanisms for international data transfers. This includes continuing to support and seek expansion of the APEC Cross Border Privacy Rules (CBPRs) system as a scalable and flexible system for ensuring the privacy of citizens' data as it crosses borders that is less burdensome to economies and companies relative to other systems. The Administration should also explore potential interoperability with other regimes such as through certification pursuant to GDPR Article 42.

3 Congress and the Administration should amend the Electronic Communications Privacy Act to require warrants for content regardless of the age of that content or the means or status of the storage of that data.

We encourage U.S. policymakers to update the outdated Electronic Communications Privacy Act (ECPA) to reflect how communications technology operates today by requiring that both law enforcement and civil agencies obtain a warrant for online content to ensure that data stored electronically and in the cloud is treated the same as data stored in the physical world, regardless of age of the content or the means or status of the storage of that data.

4 The Administration should advance policies that further the missions of law enforcement and national security entities while recognizing and supporting the critical role encryption plays in protecting individual privacy and in protecting data security.

Governments have legitimate interests in accessing data held by private entities in cases related to law enforcement and for national security purposes. Likewise, our sector has a responsibility to respect and protect the freedom of expression and the privacy of our customers; privacy, security, and personal safety are fundamental human values. The tech sector develops technology that maximizes these values. Robust cybersecurity and data protection are essential to trust in technology products, services, and systems, and robust encryption is fundamental to building trustworthy and reliable technology products, services, and systems. Issues at this intersection of privacy and security are too often portrayed in an absolutist or a binary fashion, but while distinct, privacy and security are inextricably linked in the digital world because there is no

security without privacy and there is no privacy without security. U.S. government policies should reflect this reality and recognize that U.S. policies weakening encryption would only be applicable to U.S.-based entities and their products and services, creating a market for secure competing products and services manufactured and designed by entities outside of the United States.

5 Prioritize achieving multilateral consensus (e.g. at the OECD) that reconciles law enforcement and national security processes with the protection of individual rights; pursue bilateral agreement with the EU and other qualified partners on Clarifying Lawful Overseas Use of Data (CLOUD) Act.

Globally, there is a lack of shared understanding of appropriate norms for achieving government surveillance needs while protecting individual rights; this disconnect creates significant commercial impact, including disruption to essential data flows. U.S. government commerce, law enforcement, and intelligence stakeholders should support and advance recently launched work at the OECD to identify global best practices regarding the legal bases upon which governments may compel access to personal data; requirements that meet legitimate aims and are carried out in a necessary and proportionate manner; transparency; approvals for and constraints placed on government access; limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards; independent oversight; and effective redress. Additionally, bilateral agreements with the EU and other qualified partners on the CLOUD Act are tools to facilitate modernized and efficient law enforcement access to criminal investigative information across borders. International data flows are an integral pillar of U.S. competitiveness. The State Department and DOJ should prioritize negotiating an executive agreement with the EU pursuant to the CLOUD Act, compatible with the EU's forthcoming E-Evidence Directive, to advance policies with the EU that protect national security and advance international human rights obligations, including the rights of citizens to free expression and privacy; encourage the exchange data across borders; and recognize other fundamental privacy principles such as minimization and imposing appropriate time limits on the collection and retention of personal data.

Trade

The United States is a global leader in the innovation and delivery of data-driven products and services and benefits greatly from technological innovation and digital trade. Concurrent with recent, digitally driven shifts in global trade, the United States has been a global leader in the development and international promotion of strong, state-of-the-art digital trade disciplines. Taking into account the increasingly interconnected nature of the data-driven global economy, the broadened acceptance of U.S.-style trade commitments has created positive externalities for U.S. businesses across all sectors that rely on ICT manufacturing, goods and services, and the movement of data in order to conduct their day-to-day business operations.

At the same time, U.S. trading partners, including many of its largest trading partners, continue to innovate digital policy approaches that stand to detrimentally impact not only U.S. exports but the entire global innovation ecosystem. In recent years we have seen a continued proliferation of precisely the kinds of damaging barriers to digital trade that state-of-the-art U.S. trade provisions are designed to counter. These measures have been increasingly documented by the government and the private sector, and include but are not

limited to both de jure and de facto restrictions on market access and cross-border data flows. Such restrictions inhibit value generation, reduce exports and foreign direct investment, result in productivity losses for local companies, and can have a meaningful impact on the cost and availability of key digital services. For example, specific analysis undertaken with respect to cloud services found that data-localization policies restrict access to the most cost-competitive global cloud providers, and significantly raise costs for local companies purchasing cloud-computing services.

In the face of these global policy challenges, the U.S. is well positioned to further its standing as a global leader in digital trade. ITI strongly encourages U.S. government leadership through engagement and collaboration with international partners as a primary means of countering digital protectionism and unfair trading practices, as well as broadening the acceptance of state-of-the-art commitments, including but not limited to principles and text-based approaches that facilitate the movement of data across borders, prohibit data localization, expand market access for digitally-enabled services, promote sustainability and economic inclusion, address potential market access barriers related to platform governance while enabling effective content moderation practices, and foster compatible, non-discriminatory approaches to data governance and the regulation of new technology. To this end, ITI also encourages the U.S. government to develop new mechanisms and dialogues to catalogue and challenge emerging digital restrictions, while securing commitments from other countries to avoid discriminatory or unilateral digital policies.

To guide and support robust U.S. engagement on digital trade, we make the following recommendations to ensure that companies of all sizes leveraging ICT goods and services can access and export productivity-enhancing ICT goods and services and participate in the global economy on a level playing field.

ITI Recommendations

1 Reassert U.S. commitment to the World Trade Organization (WTO).

In the first hundred days of the new Administration, USTR should signal its intent to lead in multilateral discussions at all levels of the WTO by quickly facilitating agreement on a new Director General, engaging in deliberations on WTO reform, addressing outstanding procedural impasses at the WTO, and underscoring the United States' continuing commitment to advancing commercially meaningful digital trade rules through the active participation in plurilateral negotiations on E-Commerce.

2 Reach agreement with the European Commission to stand up an EU-U.S. Trade and Technology Council.

The Administration should prioritize reaching agreement with the European Commission to stand up a transatlantic Trade and Technology Council that, among other things, would allow for discussion of digital trade and digital policy matters of interest to either party with a view to preserving an open transatlantic digital economy and enabling transparent, compatible, non-discriminatory, and innovation- and trade-facilitative approaches to digital policy at the global level. Areas of engagement should include policy approaches to AI, data governance and data-sharing, cybersecurity, cloud computing, platform governance, 5G, competition, digital taxation, digital trade commitments, and services market access. This Council could also allow for increased support for industry-led, open, voluntary, consensus-based global technical standards, including discussions with industry experts on how to align regulations and/or conformity assessment approaches with relevant standards. These discussions should also incorporate government-to-government engagement in the areas listed above as well as export controls, environment and sustainability, and countering unfair trading practices.

3 Reestablish consistent working and senior-level discussions on core issues with Chinese counterparts.

The U.S. government should reestablish consistent working and senior-level discussions on core issues with Chinese counterparts, including assessing implementation of the Phase One trade deal and benchmarks for a phased rollback of tariffs, while continuing to challenge significant outstanding concerns, such as market access restrictions on cloud and digital services. Based on progress in these discussions, USTR, Commerce, and others should establish a new, high-level effort to prioritize key bilateral issues that includes substantial industry participation.

4 Seek to broaden U.S. commercial leadership in the Asia-Pacific region and Africa.

Policymakers should comprehensively assess potential opportunities, including existing international mechanisms, for expanding acceptance of state-of-the-art rules-based commitments, eliminating barriers to trade, and strengthening relationships with strategic partners in the region. For example, the U.S. government should play a leadership role in the Asia-Pacific Economic Cooperation Forum (APEC) in expanding acceptance of digital trade commitments, eliminating barriers to digital trade, and elevating digital cooperation and regulatory compatibility as a matter of strategic importance with key partners in the region. As part of such engagement, USTR should suspend the ongoing Section 301 investigations into Vietnamese acts, policies, and practices, and any resulting actions, and address bilateral trade concerns through existing statutory and policy channels. As part of its efforts, USTR should explore a digital trade agreement with regional partners that builds on recent past initiatives incorporating state-of-the-art digital commitments. Separately, it is important for the U.S. government to support and provide capacity building assistance to the African Union as part of efforts to include a robust digital trade chapter in upcoming African Continental Free Trade Area (AfCFTA) negotiations.

5 Pursue mechanisms for expanding the acceptance of state-of-the-art digital trade commitments.

Where the United States engages with international partners in bilateral, plurilateral, or multilateral policy contexts, policymakers should prioritize broadening the acceptance of state-of-the-art digital trade commitments, principles and text-based approaches that facilitate the movement of data across borders, prohibit data localization, expand market access for digitally-enabled services, promote sustainability and economic inclusion, address potential market access barriers related to platform governance while enabling effective content moderation practices, promote innovation-oriented copyright rules, and foster compatible, non-discriminatory approaches to data governance and the regulation of new technologies in different jurisdictions. To drive engagement around forward-looking digital commitments, the Administration should complement ongoing engagement in WTO E-Commerce negotiations through defining core digital trade provisions, building on those included in recent agreements, that center on driving inclusive growth and innovation through digital trade. As part of this work, the Administration should leverage public, interagency, and Congressional input to further develop digital trade provisions that promote sustainability and inclusivity, expand good regulatory practices, limit foreign discriminatory approaches to digital regulation, and broaden the application of rules governing goods, technical regulations, technical standards, and conformity assessment to digital services.

6 Develop new mechanisms and strategies to catalog emerging restrictions and designate a senior official responsible for digital trade.

Given the evolving nature of digital restrictions globally, the Administration should initiate a comprehensive review of global digital restrictions and challenges, including an early report identifying "hot spots" of digital protectionism where current foreign digital restrictions limit the ability of U.S. companies, including small businesses, to do business and compete globally. The Administration should follow this review by articulating a digital trade enforcement strategy, outlining new steps to enforce trade agreements, and otherwise counter rising digital protectionism. Establishing a lead negotiator for digital trade with a status and mandate comparable to existing ambassador-level positions for agriculture and intellectual property, and strengthening resources at all levels of USTR, including within the digital services team, would be commensurate with the large and growing impact of digital technologies on the global economy and U.S. competitiveness and could form part of such a strategy.

International Standards

Open, industry-led international technical standards development work is a key component of trade facilitation as it enables interoperability, safety, and quality of products and services across markets. As the market leader in many current and emerging technologies, the U.S. continues to lead in international technical standards development. Yet, the international system remains hampered by countries that develop their own unique, national standards, which can become de-facto market access barriers, instead of bringing their contributions to international fora for iteration and alignment with all relevant players. In recent years the U.S. government has become overly focused on assessing international standards leadership in terms of numbers of proposals submitted by and leadership positions assigned to certain countries and companies; yet industry remains confident in international standards bodies' transparent, consensus-based processes and procedures and focuses on quality of contributions and outputs rather than quantity. This focus on quality and strategically choosing where to engage have made U.S. companies highly successful in the development of widely accepted and adopted international technology standards.

ITI Recommendations

1 Encourage countries to adopt international standards and bring their contributions to international standards bodies and deter governments (e.g., China, South Korea, India) from creating their own unique national standards.

This remains a significant problem for U.S. companies, as national standards (which are often made compulsory through adoption in law or regulation) force companies to alter their products and services to each individual market, creating market access barriers, and affecting interoperability of products and services globally. Additionally, U.S. companies may be restricted from or unable to meaningfully participate in the development of such national standards. Relatedly, ITI encourages the U.S. government to consult with technical standards experts regarding any domestic rules, regulations, or legislation that implicate standards development in order to avoid unintended negative consequences.

2 Extend Exemption of Standards Development Work from Export Controls.

In May 2020, the Department of Commerce/BIS issued a new rule clarifying that companies were not prohibited from participating in ICT-related international standards development work in fora where Listed Entity company Huawei is also present. This rule provided industry with important clarifying guidance that they would not be punished for continuing important standards leadership work, especially relevant to emerging technologies. Commerce/BIS should extend this standards-specific rule to all listed entities, so that U.S. leadership in standards development does not continue to be compromised.

Export Controls

Although export controls can be an important tool in upholding U.S. national security, so too is maintaining U.S. technological leadership, which drives U.S. innovation, job creation, and economic growth. Overly broad export controls can serve to hinder technological leadership, undermining the ability of companies to participate in the global marketplace and their ability to lead in the development of core technologies. ITI has submitted responses to both the Emerging and Foundational Technologies Advance Notice of Proposed Rulemaking which emphasize the importance of tailoring export control policies to address discrete national security risks.

ITI Recommendations

1 In implementing the Export Control Reform Act (ECRA), the Administration should prioritize engagement with multilateral export control regimes, while also considering technology areas that may be ripe for plurilateral discussions.

U.S. national security depends on the continued competitiveness of the U.S. technology industry. ITI encourages the Administration to ensure policies taken as national security measures do not inadvertently harm U.S. global competitiveness. Export controls should be narrowly tailored policies to address specific national security threats while allowing for U.S. participation in global markets, international standards development, supply chains, and R&D networks. Overly broad export controls on technology products, including through the application of unilateral controls, and other similar measures will disrupt the cycle of private-sector R&D investments made possible by revenues from sales of U.S. products to diverse customers in overseas markets. It is in this spirit that we reiterate the importance of working with industry to fully understand potential areas of concern and working with allies to administer controls that do not allow U.S. companies to be cut out of the market as unilateral controls may do.

Platforms and E-Commerce

Platforms – including e-Commerce, cloud services, B2B, B2C, search, networking, travel, and more – play a foundational role in driving technology innovation and economic growth, supporting the smooth operation of digital supply chains and creating market opportunities and access for businesses of all sizes in the tech sector and beyond. Around the world, there is a growing recognition of certain challenges and impacts, as well as a desire to advance appropriate, proportionate policy, regulatory or other instruments that could result in a consistent approach and fair competition. Proportionate instruments, where necessary, can support policymakers' goals if they focus on the specific situation, and are preceded by a consideration of whether other, less radical alternative approaches would be as effective.

As the notion of platform can refer to very different business models, policymakers should consider the role that specific companies play in the markets that they operate in, the value they create, their relationship to customers and competitors, and the possible alternatives. Grasping differences in business models and user interaction across digital platforms is key to gauging potential non-competitive conduct and properly addressing any challenges. The goal should be to maximize consumer welfare and economic efficiency, ensure market access for innovative challengers, and focus on resolving proven market failures by targeting the appropriate actions. ITI noted these considerations in detailed comments to the ongoing conversations in Europe on the Digital Services Act and Digital Markets Act.

ITI Recommendations

1 Policymakers should consider policies that promote innovation, avoid technology mandates, and enable the economic growth that platforms of all sizes have been catalysts in advancing, while also protecting freedom of expression online, advancing an environment that fosters competition, and preserving legal incentives to proactively remove harmful or exploitative material.

Relatedly, as the EU advances policies under the Digital Services Act, Digital Markets Act, and other proposals, U.S. officials should prioritize transatlantic coordination on these important topics to drive a cohesive framework that avoids fragmentation, discrimination against U.S. companies, or conflicting requirements.

2 It is crucial to coordinate efforts internationally to safeguard citizens from harmful and illegal content online (with a differentiation in approaches for illegal as opposed to harmful content) and maintain a well-functioning, competitive online ecosystem.

There is also value in exploring a more coordinated oversight model to enhance legal certainty and help companies take reasonable, feasible, and proportionate measures.

3 Any policy initiatives should be focused on the characteristics of a market and specific activities by a company, as well as objective, evidence-based economic analysis showing harm to competition and consumers.

Competition policies should focus on advancing competition and benefits to consumers, not protecting individual competitors or producers, and should not be used to further other public

policy or political interests that are more appropriately addressed in other regulatory measures. Competition policies should be objective, evidence-based, and should be designed to enhance consumer welfare. Targeting a firm based on subjective judgments about its size or conduct risks creating uncertainty, chilling innovation, and weaponizing competition law for political reasons.

4 **Proportionate instruments that advance an internationally consistent policy approach, avoid protectionism, and promote fair competition should be considered, with the goal of ensuring market access and entry for innovative challengers, safeguarding consumer welfare and economic efficiency, and addressing proven harms.**

Potential restrictions or limitations on a company's behavior or practices should be narrowly focused to achieve the intended goal.

Workforce

The competitiveness of the U.S. tech sector is dependent on its domestic workforce. Undoubtedly, innovation policy is sound workforce policy. At the end of 2019, the U.S. tech sector employed more than 12.1 million U.S. workers, was the third highest contributing sector to U.S. Gross Domestic Product (GDP) at $1.9 trillion – a full tenth of the U.S. economy – behind the manufacturing and government sectors,3 and generated the United States' 2nd and 3rd largest export of services and goods to the world, respectively, with an estimated value of $338 billion.4 Those official statistics, however, reveal only part of the positive contribution tech makes to American families and the economy. When policymakers and the public at large think of the technology sector, they often think of Austin, Boston, New York, Seattle, or northern California's Bay Area. However, the technology sector is woven throughout the country, with science, technology, engineering, and mathematics (STEM) workers and businesses in all 50 states plus the District of Columbia.

Moreover, the importance of the U.S. tech workforce has never been more evident than during the COVID-19 global pandemic. Throughout the course of the crisis, the technology sector, including American and foreign-born employees, continues to enable Americans to work and attend school remotely, and is playing an essential role in enabling the U.S. economy to move activities online and maintain vital computer and digital infrastructure to keep businesses running securely and people connected. As the country moves forward, the U.S. technology workforce will continue to be a significant component of the domestic economic recovery, including through enabling the United States to maintain its position as a global leader in innovation. As such, policymakers need to ensure that they are maximizing the full potential of current and future STEM and computer science workforce and are making the investments needed to ensure a digitally resilient workforce of the future.

ITI Recommendations

1 Policymakers should support immigration reform that successfully meets the demands of a globally competitive, digital economy by updating the H-1B visa program.

The technology sector is at the forefront of R&D investment in the United States and, subsequently, drives domestic economic growth and job creation. To achieve these objectives, tech companies rely on U.S. citizens, lawful permanent residents, and temporary non-immigrant employees educated and trained in specialized fields, as well as the ability to recruit these high-skilled professionals in the United States and globally. High-skilled immigration reform should include H-1B visa program reforms that ensure that the number of available H-1B visas adjust to meet market demands; promote additional protections for nonimmigrant employees such as H-1B portability; provide funding for domestic STEM education and training programs; and support the H-4 visa program for continued U.S. leadership on technology innovation and to bolster the U.S.' economic competitiveness.

2 Policymakers should advance legislative proposals that reform the employment-based visa program.

The race for talent is global. Many foreign, high-skilled workers have chosen the United States as their home and want to stay and continue to help grow the U.S. economy. To maximize their contributions, policymakers should actively support reforms to the employment-based visa (green card) program, which include increasing the overall number of employment-based immigrant visas available for applicants, as well as their spouses and children, such as through the recapture of unused green cards to help reduce application backlogs; eliminating arbitrary per-country caps through legislation; and exempting STEM university graduates from additional employment-based visa numerical limitations.

3 Policymakers should pass a legislative solution for Deferred Action for Childhood Arrivals (DACA) recipients.

Similar to foreign-born employees, DACA recipients are significantly contributing to the economic recovery. The Administration and Congress must ensure there is a permanent legislative solution for DACA recipients and that these individuals are afforded the protections they deserve.

4 Policymakers should support increased funding for STEM and computer science education.

In addition to meeting today's immediate tech workforce needs, the U.S. workforce must be prepared and skilled to address the demands of tomorrow to ensure the country is built back better. Policymakers should support significant funding for STEM and computer science education, which should consist of technical training for teachers; expanded access to high-quality instructional materials and rigorous STEM and computer science coursework; hands-on practical experience for students; and effective regional partnerships. Furthermore, policymakers must ensure that all students have access to high-caliber STEM and computer science education, including unrepresented minorities and girls. It is also critical to support increased funding and focus on training/upskilling programs in STEM and computer science through partnerships and other initiatives to facilitate placement of U.S. workers into digitally resilient jobs.

5 Policymakers should support apprenticeships, technical training programs in STEM and computer science, and workforce development programs with a technology focus.

Policymakers should support funding for apprenticeships (both registered and unregistered) and career and technical training programs, such as the Carl D. Perkins Vocational and Technical Training Act, which is authorized through 2024, in technology fields for Americans of all ages to take advantage of the opportunities available in our industry. It is important to ensure a range of apprenticeship models can participate (registered and unregistered) to reap the benefits of diverse offerings and the differentiated needs of students and industries. Policymakers should support further modernization of the Workforce Innovation and Opportunity Act (WIOA) to invest in workforce development and training/upskilling programs to better expand alternative career pathways to "future proof" jobs in the technology sector.

6 Policymakers should bolster federal funding for investments in Minority Serving Institutions (MSIs) and Historically Black Colleges and Universities (HBCUs).

Innovation is birthed through diverse perspectives and strategies. As such, policymakers must ensure that the STEM and computer science pipeline is accessible to and inclusive of historically disadvantaged groups to maximize the full potential of the U.S. domestic workforce who will drive the nation's economic recovery. Policymakers should prioritize federal investments in MSIs and HBCUs, which are essential for further equipping and reaching people of color and play a significant role in educating the next generation of diverse STEM and computer science professionals.

7 The Administration should strengthen the development and adoption of inclusive policies and technologies for persons with disabilities.

Digital technologies have the potential to improve education, increase employment, promote independence, and empower and improve the quality of life for persons with disabilities in America. The Administration should support initiatives which enhance the development and adoption of inclusive technologies that spur equitable innovations focused on increasing equity and opportunities for persons with disabilities.

8 The Administration should work with Congress, where there is bipartisan support for extending workplace protections to nontraditional workers.

Antiquated public and private safety nets disproportionally exclude many of the 53 million low-wage workers, 61 million workers of color, and 15 million workers in nontraditional work arrangements. Building a people-centered, tech-enabled, and interoperable system of portable benefits is critical to advancing the financial security and economic mobility of America's workers, particularly as the number of independent workers increases in the digital economy.

Broadband and Digital Infrastructure

As COVID-19 has shifted many parts of daily American life online, connectivity has become an absolute necessity for American families, students, businesses, and communities. While the United States has made strides in bridging the digital divide, there are still nearly 19 million Americans without access to high-speed internet. Federal investment in secure connected infrastructure is critical to bridging the digital divide and expanding broadband access. In the future, the importance of digital technologies will only increase because they are also critical for the flexible grids and smart adaptive products, technologies, and services that are essential for the transition to a low carbon economy.

ITI Recommendations

1 Policymakers should set a goal of making high-speed broadband and 5G available to all Americans within 5 years and commit at least $80 billion in secure broadband infrastructure funding.

Public funding should be targeted to complement private sector investments and speed up both broadband and 5G roll out. Deploying secure 5G networks and ensuring ubiquitous access to connectivity will require additional measures, including improving mapping availability, streamlining permitting and other regulatory barriers to facilitate small cell deployment for 5G, and ensuring the necessary workforce for 5G deployment, including tower technicians. We encourage policymakers to leverage the 5G Policy Principles for Global Policymakers that ITI released earlier this year, which provide recommendations that cover everything from innovation and investment to 5G security, as well as a companion explainer document that helps lend context to our recommendations and debunks common myths.

2 Policymakers should pursue policies that reduce barriers to broadband adoption in order to close the digital divide and the homework gap.

Congress and the Administration should prioritize broadband adoption through expansion of the E-Rate program, initiatives that defray the cost of users' equipment, public-private partnerships to fund broadband infrastructure for unserved and underserved communities, and education-focused access programs like WiFi hotspots and laptops to students who qualify for subsidized school lunch programs.

3 Policymakers should promote increased commercial use of spectrum to connect more Americans to high-speed wireless networks and accelerate the deployment of 5G.

More spectrum, including licensed, unlicensed, and shared-use and particularly in the mid-band will be necessary to fuel 5G networks, and policymakers should advance shared-use policies that expand commercial spectrum opportunities and increase availability of spectrum.

4 Policymakers should improve resiliency through the deployment and integration of smart technologies into the design, construction, and use of traditional infrastructure and transportation systems and IT modernization.

Supporting IT modernization and incorporating emerging technologies, through smart, secure, data-driven, standards-based Internet of Things (IoT) and operational technology (OT) solutions, into the design, construction, and foundation of any new, or repairs of existing, infrastructure – from roads, bridges, and traffic management and transportation systems, to the electric grid, communications network, and water infrastructure

– will improve public safety, reduce congestion, conserve energy, maximize efficiency, save significant taxpayer dollars, be more sustainable and environmentally-friendly, and enhance overall quality of life.

5 Policymakers should support open and interoperable solutions for 5G networks, especially through allocating additional funding for R&D in this area.

Networks built on open standards will allow for interoperability and increase competitiveness, innovation and supplier diversity on a massive scale. As the United States seeks to build out secure 5G networks, it is important to consider new and innovative technology solutions as a way to address some of the challenges that have been identified in the National Strategy to Secure 5G. The best way to maximize the benefits of new technologies is to promote a competitive marketplace and let market forces work. Therefore, the Administration should support a technology-neutral environment that promotes innovation, allowing the private sector to lead and the market to determine the "winners."

6 Policymakers should address deficiencies in our digital identity infrastructure.

The benefits of a digital economy begin and end with trust. The COVID-19 pandemic has laid bare the inadequacies of the nation's digital identity infrastructure, as many in-person services have been eliminated and many could not be replicated online due to insufficient identity verification and authentication solutions. The majority of services in today's economy – from healthcare to banking to online commerce – depend on knowing "who is on the other side" of a transaction. Traditionally, identification has been anchored in the physical world, such as presenting a passport, proof of address, or driver's license in person. These forms of identificationare insufficient in a digital environment. This disconnect creates friction in an online environment, leads to increased fraud and theft, and degrades privacy. Together, government agencies and the private sector could drive significant risk and fraud out of online services and allow all citizens to more easily and securely engage in transactions online. More could be done to find secure, user-friendly, and privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market.

7 Policymakers should incentivize manufacturing of advanced semiconductors in the United States.

Revitalizing high-tech manufacturing of semiconductors in the United States has the potential to drive innovation across many different sectors for decades to come. For example, semiconductors drive advancements in AI, quantum computing, medical technologies, and 5G—the horizontal technologies driving the data-driven innovative and technological growth and development enriching U.S. society and economy. Semiconductor leadership drives the resiliency and competitiveness of the U.S. digital supply chain, ICT sector, and the economy at large. Investing in large-scale missions—like ushering in a silicon manufacturing renaissance—would restore American leadership in advanced manufacturing, secure these vital supply chains, grow well-paying jobs, and ensure our technological long-term national security and economic competitiveness. The Administration should also pair these incentives with funding for research, development, testing, and evaluation of projects and activities related to semiconductors and other components critical to the broader high-tech ecosystem.

Digital Government Services

It is imperative that American technological leadership and innovation is leveraged by government to modernize and improve the U.S. public sector's information technology (IT) and cybersecurity in ways that improve and revolutionize the delivery, security, and efficiency of digital government services. The pandemic has reinforced what years of more gradual change has made clear — that resilient, more capable, efficient, and economical IT systems, and more effective means of protecting them against cyber threats, are necessary.

The reality is that many of the systems that government still uses today are years, if not decades, old, and the government has made slow progress toward its digital transformation. The government systems are limited in the elasticity of their capabilities, have become very costly to maintain and evolve, and in some agencies, are not at all well positioned for the challenges or changes anticipated in the future. Obsolete and legacy systems require greater maintenance, are more difficult to adapt to meet new needs, and the costs associated with them increasingly crowd out resources that should be invested in better, more capable, and less costly modern systems that are more easily adapted. Additionally, failure to achieve a fully digital government will continue to impact government services and divert resources toward antiquated processes. Improved government technology and cybersecurity is crucial to providing Americans the government services they seek and need, through current and future acute challenges, like COVID-19, in ways that evolve with changing initiatives and evolving expectations, and that preserve and help to restore trust in government. Further, government entities, as authoritative issuers of identity in America, are uniquely positioned to deliver critical components that address deficiencies in our nation's digital identity infrastructure. In doing so, much more could be done to find secure, user-friendly, and privacy-centric ways in which government could modernize the delivery of and access to government services to citizens.

Technology solutions and the resilience of the technology manufacturing supply chain can boost US competitiveness by enabling the U.S. government to deliver superior services to Americans. When governments select the right tools, they will improve the delivery of services to their constituents and strengthen democratic processes. Complacency, on the other hand, will erode them over time. Currently, the federal government spends approximately 80 percent of its nearly $90 billion annual IT budget on the maintenance and operation of legacy networks and systems. These funds should be redirected and increased to hasten strategic modernization efforts of federal IT infrastructure.

ITI Recommendations

1 Policymakers should work with Congress to provide increased funding for strategic IT modernization investments and supply chain resiliency.

Meaningful and significant boosts in agency technology budgets as well as more robust funding and policy changes for dedicated government-wide IT efforts like the Technology Modernization Fund (TMF) are necessary. These funds should be used for foundational investments in cyber and technology modernization to retire obsolete legacy systems and better prepare our country to recover from the pandemic stronger than we were before and serve us for years to come. Without meaningful investments in modernizing government IT and cybersecurity at all levels of government, the costs to keep limited and unsecure systems going will continue to rise, which would leave even less to invest in new IT and respond to unforeseen emergencies.

2 Policymakers should reform the cybersecurity policy landscape.

Streamlining and harmonizing the existing piecemeal approach to cybersecurity policies will enable government to leverage the best available cyber defensive capabilities and provide government leadership with the information needed to make informed, risk-based decisions on security. Deficiencies in federal IT security put government's and Americans' information at risk, undermine the effectiveness of new and ongoing government operations, and threaten the security of our country. Aligning government cybersecurity requirements with the NIST Framework for Improving Critical infrastructure Cybersecurity (CSF) can help enable greater efficiency, competition, and scale. Relevant existing laws and regulations include but are not limited to the Federal Information Security Management Act (FISMA), the Federal IT Acquisition Reform Act (FITARA), the Federal Risk and Authorization Management Program (FedRAMP), the Internet of Things (IOT) Cybersecurity Improvement Act, and the Cybersecurity Maturity Model Certification (CMMC) at the Department of Defense. Such reforms should focus on incorporating security policy best practices such as facilitating interoperability, leveraging existing international and industry standards, and avoiding duplicative requirements that may stifle the development and adoption of innovative technologies.

3 Policymakers should support increased investments in government cybersecurity at both the Federal and State, Local, Tribal, and Territorial (SLTT) levels.

The Continuous Diagnostics and Mitigation (CDM) program is the primary federal government initiative for protecting civilian federal agencies. Robust investment in the CDM and other federal cybersecurity programs will be critical for securing the delivery and efficiency of digital federal services. SLTT governments are facing increasing service delivery and cybersecurity challenges made worse by malicious cyber actors who have used attention on COVID-19 to their advantage, targeting SLTT government and individual citizens with ransomware, phishing, and computer-enabled financial fraud. It is critical that the Administration make the necessary and profoundly important investments in the modernization and security of SLTT information systems so they can protect citizen data, improve digital services delivery, and ensure that state and local governments have the necessary tools to protect against cyber-attacks.

4 Policymakers should increase competition and innovation within the government procurement process.

Government procurement policy should be enhanced to prioritize laws, regulations, policies and programs that streamline the acquisition of commercial items, commercially available off-the-shelf products (COTS) and "as a service" (aaS)" offerings. Such a reform strategy should leverage private sector innovation and foster competition by avoiding government- or agency-unique requirements or the favoring brand names without justification. To expedite the roll-out process, government officials should consider and grant additional flexibilities in the acquisition of innovative technologies. A streamlined procurement process will maximize competition and improve governmental mission delivery.

5 Policymakers should improve secure access to public data.

To leverage the wealth of information collected by government agencies on social and economic issues, government agencies should promote the use of and provide access to public data. Interoperability of government data is essential so that information is not only collected but is also accessible to the public. Leveraging data transparency enables the development of AI-based tools that aid users in analysis and problem solving at speed and scale. Standards for federal and state agencies on open data and web APIs may be effective at achieving this goal. The Administration can also invest in shared data platforms, both within and across government agencies, to streamline public access and reduce fragmentation of various sources of government information. By supporting the National AI Initiative and the Executive Order Promoting the Use of Trustworthy AI, the Administration can ensure that government agencies have the right AI-based tools to solve hard problems using these data.

6 Policymakers should assert renewed strong science-based climate policy leadership from Washington.

Technology and data offer new tools to contribute to the achievement of climate ambitions. The ICT sector stands ready to support technical assistance and capacity building efforts that will be necessary to achieve a low-carbon future. This is critical for the future of humanity, and it will also spur economic growth, create jobs, improve health, and enhance the overall quality of life.

www.itic.org