

**Date:** December 6, 2024

**To:** President-Elect Donald Trump  
Policy Advisor

**From:** ACT | The App Association

**Re:** Policies and Actions to Support American Small Businesses in the Trump-Vance Administration

ACT | The App Association congratulates you on your victory in the 2024 election.

The App Association is a policy trade association representing the small business technology developer community. Our members are entrepreneurs, innovators, and independent developers located across the United States that compete across consumer and enterprise markets. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology.

The value of the ecosystem the App Association represents—which we call the app economy—is approximately \$1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the \$8 trillion internet of things (IoT) revolution.<sup>1</sup> App Association members are key drivers of a broader U.S. digital economy that, on its own, is the world's eighth-largest economy. Yet our members' ability to grow and create American jobs faces significant challenges, exacerbated in some cases by either inaction or ill-advised policies during the previous Administration, that now represent immense opportunities for the Trump-Vance Administration.

Since its founding, the App Association has been, and remains, committed to American small business growth and job creation. Today, the app economy is an incredible means of innovation, creativity, and empowerment that must be supported through both domestic and international policies. Below, we elaborate on these opportunities and make targeted recommendations on how the incoming Trump-Vance Administration can positively impact the economic prosperity of ordinary Americans across the country across the following areas:

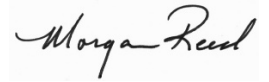
- Competition
- Artificial Intelligence
- Intellectual Property Rights
- Broadband and Telecommunications
- Cybersecurity
- Privacy
- Trade and Market Access Abroad
- Standards

---

<sup>1</sup> ACT | The App Association, State of the App Economy (2022), <https://actonline.org/wpcontent/uploads/APP-Economy-Report-FINAL.pdf>.

We welcome the opportunity to meet with you to share further perspectives and recommendations that will contribute to reclaiming American growth, job creation, and leadership.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is written in a cursive style with a large, prominent 'M' and 'R'.

Morgan Reed  
President

## Executive Summary

This memo outlines the App Association's strategic recommendations for the Trump-Vance Administration to enhance American small business growth and job creation through a focus on key areas of policy, including competition, artificial intelligence (AI), intellectual property (IP), broadband and telecommunications, and cybersecurity. Notable recommendations include:

**Competition:** We advise against expanding the application of antitrust laws in a manner that would harm small businesses relying on online marketplaces and across emerging and nascent technology-driven markets. We also urge a significant departure from the DoJ's approach to antitrust cases against Apple and Google, as these actions could harm small businesses that benefit more than their larger rivals from marketplace management.

**Artificial Intelligence:** We recommend a coordinated federal approach to AI regulation, emphasizing innovation and alignment with NIST's AI Risk Management Framework. We strongly discourage efforts to regulate AI technology specifically and instead recommend intervention only where observed harms may be addressed by government action and where its costs are outweighed by the benefits of such intervention.

**Intellectual Property Rights:** We recommend a range of measures that should be taken to support U.S. economic growth and security through U.S. intellectual property rights policies. Notably, such measures should include taking steps to confront standard-essential patent (SEP) abuse to protect national security and bolster American competitiveness in technology markets.

**Broadband and Telecommunications:** We highlight the need for accurate broadband mapping and streamlined infrastructure deployment to bridge the digital divide and support small business growth.

**Cybersecurity:** We support a risk-based approach to dynamic cybersecurity threats, which recognizes the importance of technical protection mechanisms like strong encryption to protect small businesses from cyber threats.

**Privacy:** We call for the Administration's support for legislation creating a federal data privacy framework with strong preemption of state laws, a path to compliance for small businesses, and enforcement focused on specific harms so as not to stifle innovation.

**Trade and Market Access Abroad:** A renewed focus on enabling American small businesses to compete and succeed abroad through U.S. trade policy is sorely needed. The Administration must reclaim leadership in championing pro-digital trade policies that have fostered the growth of the U.S. small business digital economy.

**Standards:** The Administration's leadership is needed to support open, private sector-led standards processes that enable the U.S. to lead globally while engaging constructively with international partners.

Taken together, the App Association's recommendations offer a roadmap for U.S. growth, competition, and innovation through support for small businesses in a rapidly evolving technological landscape.

## ACT | The App Association's Recommendations for Renewed American Growth and Job Creation

### Competition

The App Association shares the Trump-Vance Administration's goals of supporting competition and innovation across technology-driven markets, which is critical for reclaiming American growth, job creation, and leadership. The use of competition law can have profound impacts, and it is vital that U.S. competition policy maintain a deference to thorough economic analysis as a foundation and ensure that interventions and enforcements occur in response to demonstrated systemic harms (not edge use cases or hypotheticals).

The Biden-Harris Administration sought unprecedented expansions to the scope of antitrust law to target online marketplaces. These ideas can be difficult to resist, since they appear at first to address some of the popular complaints about large tech companies. The largest companies (some of which fall outside the commonly used list of "Big Tech" firms) doing business on those platforms have seized the opportunity to gain an advantage through such government interventions,<sup>2</sup> which would harm the smallest companies distributing goods and services on online marketplaces. The online marketplace model is one that has directly supported entrepreneurship and innovation for small businesses by providing distribution options that (1) lower overhead costs, (2) provide one-stop access to global markets, and (3) deliver instantaneous consumer trust. Accordingly, the Trump-Vance Administration should avoid efforts to illegalize or otherwise target small business-friendly aspects of online marketplaces, such as the wraparound services and centralized distribution they provide.

We strongly urge the Trump-Vance Administration to consider the outcomes should it press forward with the previous Administration's antitrust agenda, namely that American businesses' ability to compete, both domestically and internationally, will be significantly undermined. Opening the door for foreign adversaries to step in and fill this vacuum will directly harm the American economy and its national security.

#### *1. Department of Justice (DoJ)*

During the Biden-Harris Administration, DoJ sought to expand the scope of antitrust law to protect competitors—rather than competition and consumers—by seeking outlandish remedies in its Google search case and by challenging the very ecosystem management decisions Apple makes that small businesses find most attractive.

**The Apple case.** DoJ alleges that Apple monopolized the market for "performance smartphones" by restricting access to its hardware and software to protect privacy, security, and the value of the platform. In each of its claims, DoJ takes the side of the largest companies doing business on Apple's platform, from Bank of America to Meta. If DoJ prevails, the restrictions that are most useful for small businesses—albeit inconvenient for the largest companies—would be declared illegal. Small business app makers benefit more than their larger competitors from the fact that Apple cultivates a

---

<sup>2</sup> See "Antitrust Applied: Examining Competition in App Stores," hearing before the U.S. Senate Subcommittee on Competition Policy, Antitrust, and Consumer Rights, Apr. 21, 2021 (testimony of Spotify, Match Group, Inc., and Tile, Inc.).

privacy- and security-protective ecosystem. By declaring restrictions that limit open access illegal, a DoJ win would hurt small businesses while helping larger rivals. The Trump-Vance DoJ should decline to pursue this lawsuit any further.

**The Google search case.** In a case initially brought by the first Trump Administration, the District Court ultimately found Google liable for monopolization by entering into default agreements with browser and device makers. Unfortunately, the Biden-Harris DoJ has taken the opportunity to centrally plan what is currently a dynamic set of digital markets. In its proposed remedies, DoJ indicates its intent to ask for parts of Google to be broken up and for access to search data to be made free and commoditized, even going so far as to bar Google from competing or investing in artificial intelligence (AI) markets. Small app companies benefit immensely from Google's significant investments in AI, its robust search advertising offerings, and its managed Google Play marketplace. The last thing they want is for the government to devalue Google's offerings and shut off AI investment so that weaker competitors and shallower pockets have a shot. Competitors should have to beat Google on the merits. If antitrust policy pursues the lowest common competitive denominator, small app companies will suffer from worse app store management, less investment in the AI services they purchase, and less powerful advertising and search options. The Trump-Vance DoJ should withdraw these proposed remedies as the lower court decision is appealed.

The Trump-Vance Administration's DoJ should carefully consider the next steps it takes in addressing competition policy and the law's application to emerging and nascent technology-driven markets. **To protect the United States economy and national security, the Trump-Vance Administration should (1) withdraw existing ill-advised antitrust lawsuits against American companies that would negatively disrupt the foundations on which U.S. small business growth and job creation have been built; and (2) combat foreign jurisdictions' imposition of anti-U.S. discriminatory regulations intended to lock out American competitors.**

## *2. Unprecedented Proposed Changes to Antitrust Laws*

Congress has recently considered two antitrust-related bills that would target online marketplaces: the American Innovation and Choice Online Act (AICOA) and Open App Markets Act (OAMA). These bills would significantly harm the prospects of small app companies that leverage online marketplaces by 1) presumptively outlawing "self-preferencing," which would discourage or outright ban wraparound services like privacy controls, developer tools, and access to application programming interfaces (APIs); and 2) presumptively requiring open access to the marketplaces, which would discourage or outright ban removal of problematic content like malware, copycat, or fraudulent apps from those marketplaces. These policy approaches would significantly undermine the three-prong value our member companies derive from online marketplaces:

1. The provision of a bundle of services that reduces overhead costs;
2. Instantaneous and cost-effective consumer trust mechanisms; and
3. Cost-effective access to a global market.

Unfortunately, in their pursuit of creating advantages for select competitors, the bills would also harm consumer protection efforts and protections in place on online marketplaces. We detailed these issues in letters to the congressional committees of jurisdiction and explained how undermining privacy, security, and safety on the marketplaces disproportionately harms the smaller companies leveraging those marketplaces for distribution.<sup>3</sup> **We strongly urge the Trump-Vance Administration to oppose legislation that would short-circuit competition analyses that must serve as the foundation for any government intervention on antitrust grounds, particularly for emerging and nascent markets that App Association members focus on.**

### 3. *The Federal Trade Commission (FTC)*

The FTC’s campaign to eliminate the online marketplace model undermines American economic growth and leadership on the global stage. As we testified before the Senate Antitrust Subcommittee in March of 2020, the online marketplace practice of providing wraparound services is a procompetitive example of “self-preferencing” and should not be eliminated by legislation or overly aggressive antitrust enforcement.<sup>4</sup> Likewise, we described the value that small businesses in particular—in contrast with larger companies petitioning the Subcommittee to intervene—derive from digital marketplaces.

Unfortunately, the FTC has deprioritized these considerations. Over the past four years, the FTC has applied its antitrust authority primarily to advantage competitors rather than competition and consumers. It has pursued this agenda in several ways:

- Adopting a Section 5 Unfair Methods of Competition Enforcement Policy statement declaring a wide range of procompetitive conduct potentially illegal;
- Adopting a set of anti-small business joint merger guidelines and extreme pre-merger filing requirements with the U.S. Department of Justice (DoJ) declaring a broad set of procompetitive mergers potentially illegal;
- Adopting several anti-merger policies, including proposing merger review rules that would increase compliance costs by orders of magnitude for companies seeking to be acquired, effectively closing off pathways to success for small, innovative companies;
- Suing Amazon for a set of small business- and consumer-friendly online marketplace practices; and
- Successfully petitioning the United States Trade Representative (USTR) to abandon small business-friendly digital trade priorities and colluding with European officials responsible for the protectionist Digital Markets Act (DMA) to strengthen the FTC’s domestic anti-small business enforcement campaign.

---

<sup>3</sup> See, e.g., Letter from Morgan Reed, president, ACT | The App Association, to Senate Judiciary Committee leadership re: “Reining in Dominant Digital Platforms: Restoring Competition to our Digital Marketplace,” (Mar. 6, 2023), *available at* [link]; Letter from Morgan Reed, President, ACT | The App Association to U.S. Senate leadership, re: Open App Markets Act (S. 2710) and American Innovation and Choice Online Act (S. 2992) Would Create Unacceptable New Threat Vectors in Mobile Ecosystems, (Mar. 8, 2022), *available at* <https://actonline.org/wp-content/uploads/2022-03-08-ACT-Ltr-to-Senate-re-OAMA-AICOA-Mobile-Threats57.pdf>.

<sup>4</sup> “Competition in Digital Technology Markets: Examining Self-Preferencing by Digital Platforms,” Hearing before the U.S. Senate Judiciary Comm., Subcomm. on Antitrust, Competition, and Consumer Rights (116th Cong., 2d Sess.), Mar. 10, 2020 (statement of Morgan Reed, President, ACT | The App Association), *available at* <https://actonline.org/wp-content/uploads/2020-03-07-ACT-Testimony-Senate-Judic-Antitrust-Sub-Hrng-FINAL.pdf>.

This is not an exhaustive list of FTC activities that would undermine the success of small businesses across the nation. **We urge the Trump-Vance Administration to ensure that candidates for FTC leadership oppose overreaching enforcement and policy approaches like the FTC’s recent efforts during the Biden-Harris Administration.**

## **Artificial Intelligence**

AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking – learning and reasoning among them. An encompassing term, AI entails a range of approaches and technologies, such as Machine Learning (ML) and deep learning, where an algorithm is based on the way neurons and synapses in the brain change due to exposure to new inputs, allowing independent or assisted decision making. AI-driven algorithmic decision tools and predictive analytics are having, and will continue to have, substantial direct and indirect effects on Americans. Some forms of AI are already in use to improve American consumers’ lives today; for example, AI is used to detect financial and identity theft and to protect the communications networks upon which Americans rely against cybersecurity threats.

Across use cases and sectors, AI has incredible potential to improve American consumers’ lives through faster and better-informed decision-making enabled by cutting-edge distributed cloud computing. As an example, healthcare treatments and patient outcomes stand poised to improve disease prevention and conditions, as well as efficiently and effectively treat diseases through automated analysis of X-rays and other medical imaging. AI will also play an essential role in self-driving vehicles and could drastically reduce roadway deaths and injuries. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions. Americans already encounter AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition (we urge consideration of these forms of AI as “narrow” AI); meanwhile, generative AI tools are revolutionizing, and will continue to revolutionize, each consumer and enterprise sector/use case.

The App Association encourages the Administration to support a coordinated effort to harmonize the use of AI across both executive and independent agencies. As a result of the Biden-Harris Administration’s AI Executive Order, numerous regulatory agencies, some cross-sectoral and others sector-specific, have considered or advanced regulatory proposals that would take starkly different approaches to AI accountability. Some of these proposals have put significant hurdles in place for the development and use of AI through approaches that have little-to-no public benefit. In some cases, such proposals have been developed based on speculative and undemonstrated harms. The Trump-Vance Administration must seize its opportunity to reorient the federal government’s approach to one that promotes innovation and celebrates American success.

Many entities, both public and private, are actively engaging in efforts to create and enforce AI accountability frameworks, which may lead to the creation of trusted audits, assessments, and certifications. While this area continues to evolve, we strongly urge the Trump-Vance Administration’s approach to AI governance to align with NIST’s AI Risk Management Framework, which aims to help designers, developers, users, and evaluators of AI systems evolve in knowledge, awareness, and best practices to better manage risks across the AI

lifecycle.<sup>5</sup> NIST's AI RMF is best positioned to guide efforts across the federal government in addressing AI due to NIST's expertise and its collaborative and open approach to developing the AI RMF, similar to NIST's Cybersecurity Framework.<sup>6</sup> It is in the public's best interest that the NIST AI RMF's scaled, risk-based approach serve as a basis for both executive and independent agencies' approach to AI risk management and governance, and that federal agencies take active steps to bring themselves into alignment with this approach. Further, we call on the Trump-Vance Administration to prioritize the impact of their AI regulatory efforts on small businesses that drive innovation and competition across consumer and enterprise markets.

**We strongly encourage the Trump-Vance Administration's AI-related efforts to align with the following principles:**

### **1. Harmonizing and Coordinating Approaches to AI**

A wide range of federal, local, and state laws prohibit harmful conduct regardless of whether the use of AI is involved. For example, the Federal Trade Commission (FTC) Act prohibits a wide range of unfair or deceptive acts or practices, and states also have versions of these prohibitions in their statute books. The use of AI does not shield companies from these prohibitions. However, federal and state agencies alike must approach the applicability of these laws in AI contexts thoughtfully and with great sensitivity to the novel or evolving risks AI systems present. The administration must first understand how existing frameworks apply to activities involving AI to avoid creating sweeping new authorities or agencies that awkwardly or inconsistently overlap with current policy frameworks.

### **2. Quality Assurance and Oversight**

Policy frameworks should utilize risk-based approaches to ensure that the use of AI aligns with any relevant recognized standards of safety and efficacy. Small software and device companies benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so. Some recommended areas of focus include:

- Ensuring AI is safe and efficacious.
- Encouraging AI developers to consistently utilize rigorous procedures and enabling them to document their methods and results.
- Encouraging those developing, offering, or testing AI systems intended for consumer use to provide truthful and easy-to-understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.

---

<sup>5</sup> <https://www.nist.gov/itl/ai-risk-management-framework>.

<sup>6</sup> <https://www.nist.gov/cyberframework>.



### **3. Thoughtful Design**

Policy frameworks should encourage design of AI systems that are informed by real-world workflows, human-centered design and usability principles, and end user needs. AI systems should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should leverage collaboration and dialogue among users, AI technology developers, and other stakeholders to have all perspectives reflected in AI solutions.

### **4. Access and Affordability**

Policy frameworks should enable products and services that involve AI systems to be accessible and affordable. Significant resources may be required to scale systems. Policymakers should also ensure that developers can build accessibility features into their AI-driven offerings and avoid policies that limit their accessibility options.

### **5. Bias**

The bias inherent in all data, as well as errors, will remain one of the more pressing issues with AI systems that utilize machine learning techniques. Regulatory agencies should examine data provenance and bias issues present in the development and uses of AI solutions to ensure that bias in datasets does not result in harm to users or consumers of products or services involving AI, including through unlawful discrimination.

### **6. Research and Transparency**

Policy frameworks should support and facilitate research and development of AI by prioritizing and providing sufficient funding while also maximizing innovators' and researchers' ability to collect and process data from a wide range of sources. Research on the costs and benefits of transparency in AI should also be a priority and involve collaboration among all affected stakeholders to develop a better understanding of how and under which circumstances transparency mandates would help address risks arising from the use of AI systems.

### **7. Privacy and Security**

The many new AI-driven uses for data, including sensitive personal information, raise privacy questions. They also offer the potential for more powerful and granular privacy controls for consumers. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. A balanced framework should avoid undue barriers to data processing and collection while imposing reasonable data minimization, consent, and consumer rights frameworks.

## **8. Ethics**

The success of AI depends on ethical use. A policy framework must promote many of the existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. Relevant ethical considerations include:

- Applying ethics to each phase of an AI system's life, from design to development to use.
- Maintaining consistency with international conventions on human rights.
- Prioritizing inclusivity such that AI solutions benefit consumers and are developed using data from across socioeconomic, age, gender, geographic origin, and other groupings.
- Reflect that AI tools may reveal extremely sensitive and private information about a user and ensure that laws require the protection of such information.

## **9. Education**

Policy frameworks should support education for the advancement of AI, promote examples that demonstrate the success of AI, and encourage stakeholder engagements to keep frameworks responsive to emerging opportunities and challenges.

- Consumers should be educated as to the use of AI in the service(s) they are using.
- Academic education should include curriculum that will advance the understanding of and ability to use AI solutions.

## **10. Intellectual Property**

The protection of intellectual property (IP) rights is critical to the evolution of AI. In developing approaches and frameworks for AI governance, the Administration should ensure that compliance measures and requirements do not undercut IP or trade secrets.

### **Intellectual Property Rights**

Intellectual property (IP) rights protect innovation and are vital to supporting American growth and job creation. Members of the App Association, both securing and licensing IP, depend on a balanced and reliable IP framework to support their efforts to compete and grow.

The Biden-Harris Administration left countless opportunities to advance pro-competitive and pro-small business IP policies on the table and demonstrated little interest in even addressing IP issues meaningfully. As a prime example, the Biden-Harris Administration never appointed an Intellectual Property Enforcement Coordinator (IPEC) in the White House over their four years in power. The Trump-Vance Administration now has the opportunity to take action and address these opportunities. Reclaiming American growth, job creation, and leadership will require focused and coordinated action by the Trump-Vance Administration on a range of IP issues across all areas of IP (patents, copyrights, trademarks, and trade secrets).

## A. Patents

Patents serve as a mechanism to protect a novel, non-obvious, and industrially applicable idea or process. Small business innovators both hold and license patents, and a fair and consistent patent process is critical to innovation. As more devices throughout the consumer and enterprise spheres become connected to the internet— often referred to as the internet of things (IoT) — App Association members' innovations will remain the interface for communicating with these devices. Small business viability is directly correlated to fairness and predictability in the patent system.

The Trump-Vance Administration is well-positioned to provide needed leadership in patent policy, which will support American growth and leadership.

The United States Patent Office (USPTO or the Office) issues well over 300,000 patents a year, of which a significant amount are overly vague and/or obvious (e.g., almost 90 percent of the patents that are challenged at the Patent Trial and Appeal Board [PTAB] are found to be invalid upon review. Many of these poor-quality patents are held by foreign adversaries and their proxies and are unreasonably and frivolously enforced against small businesses that cannot afford the costs of litigation and are therefore forced to settle on unreasonable terms that tax their innovative efforts and ability to hire.

The USPTO has identified that foreign abuse is prevalent in the U.S. patent system and a large concern for stakeholders. Foreign entities that are issued U.S. patents use venues like the International Trade Commission (ITC) and the federal courts to assert infringement claims against innovators. The ITC is particularly attractive to abusers of the patent system because parties are not required to follow certain procedures, and the agency can only award exclusion orders. Foreign companies have enforced invalid and overbroad patents and, in some cases, have taken the form of non-practicing entities (NPEs) backed by third-party litigation funding (TPLF).

**The Trump-Vance Administration should take immediate steps to support American small business innovation and job creation by:**

- **Ensuring the USPTO takes new and targeted steps to ensure that it issues valid patents in order to prevent patent trolling, particularly by foreign adversaries or their proxies;**
- **Supporting a reliable and transparent PTAB process for all small businesses that will remove weak and invalid patents that should never have been issued in the first place; and**
- **Taking immediate action to expose and eliminate TPLF by foreign entities and their proxies who seek to profit from gaming the U.S. patent system.**

### **a. Standard-Essential Patents**

Sitting at the intersection of patent rights, competition law, and standards policy, abuse of the standard-essential patent (SEP) ecosystem represents an immediate and significant threat to the U.S. economy and national security. Action to support a balanced approach to SEP licensing through policies and enforcement is critical to supporting U.S. small business innovation across technology-driven markets and to the economy and national security writ large.

The goal of establishing technical standards is to provide an efficient and interoperable base for technology developers to create new inventions across multiple market sectors. When a patent holder contributes their technology to a technical standard, they understand and agree that they

are using their patent to enable reasonable access to the standard and provide standard-setting organization (SSOs) with a commitment that they will license their SEPs on fair, reasonable, and non-discriminatory (FRAND) terms to balance against the anticompetitive risks associated with standard setting. Therefore, by contributing to the standardization process, a SEP holder understands and agrees to not unduly exclude competitors from a standard past requiring a FRAND license.

Recognizing how easily a SEP holder can make FRAND promises and then later obfuscate and disregard them, a growing number of foreign companies have turned SEP licensing into a business that, at its base, is predation of good faith innovators and small companies who simply need to use standardized solutions to compete. And their efforts have, in part, been successful. Today's framework of SEP laws and policies, both in the United States and abroad, unduly favor these foreign SEP holders by, for example, enabling systematic seeking of prohibitive orders in other important jurisdictions on FRAND-committed SEPs before a court would assess the validity or essentiality of the SEP at issue. Such practices have long taken place in telecommunications markets and are now finding their way into new verticals where connectivity is being built into consumer and enterprise products, such as automotive and medical. Such unchecked practices already translate to limited availability and higher prices for Americans (to the benefit of foreign adversaries and their proxies), undermining a core goal for the Trump-Vance Administration.

ACT | The App Association believes that clear guidance is needed to prevent foreign entities and their adversaries from holding technical standards hostage by way of anticompetitive standard-essential patent (SEP) licensing practices. Standards support U.S. small business innovation in emerging technology and provide American consumers with ample low-cost market alternatives.

American innovation in emerging technology often involves the inclusion of consensus-based and industry-led technical standards, such as 5G and Wi-Fi. These standards have been applied to critical internet of things (IoT) and artificial intelligence (AI) while impacting industries, including automotives and healthcare. The goal of establishing technical standards is to provide an efficient and interoperable base for technology developers to create new inventions across multiple market sectors. When a patent holder contributes their technology to a technical standard, they understand and agree that they are using their patent to enable reasonable access to the standard and provide standard-setting organizations (SSOs) with a commitment that they will license their SEPs on fair, reasonable, and non-discriminatory (FRAND) terms to balance the anticompetitive risks associated with standard setting. Therefore, by contributing to the standardization process, a SEP holder understands and agrees to not unduly exclude competitors from a standard past requiring a FRAND license.

### ***China Has Empowered Its Domestic Businesses To Weaponize SEP Licensing Against American Companies***

China has already demonstrated its willingness to weaponize the standards and intellectual property (IP) systems to disadvantage the American economy, national security, and American companies (e.g., its development of the WLAN Authentication and Privacy Infrastructure (WAPI) Chinese national standard to undermine Wi-Fi and restrict access to the Chinese market<sup>7</sup>). Recognizing how easily a SEP holder can make FRAND promises and then later obfuscate and disregard them, a growing number of companies, including those controlled by foreign

---

<sup>7</sup> <https://actonline.org/2016/03/17/mobile-mythbusting-wifi-wapi-and-the-encryption-debate/>.

adversaries, namely China—have turned SEP licensing into a business that, at its base, is predation of good faith American innovators and small companies who simply need to use standardized solutions to interoperate and compete. And their efforts have, in part, been successful. Today's framework of SEP laws and policies, both in the United States and abroad, unduly favor these foreign adversaries and their proxies that hold key SEPs by, for example, enabling the locking out of U.S. competitors from entering entire markets. Even more concerning, foreign adversaries' strategic decision to accumulate key technology patents and insert them into key standards as essential throughout global supply chains, presenting a direct economic and national security to the United States.

The SEP licensor abuse playbook is well-practiced. SEP abuses have taken place in telecommunications markets (for well over 20 years) and are now finding their way into new verticals where connectivity is being built into consumer and enterprise products, such as automotive and medical. Such unchecked practices already translate to limited availability and higher prices for Americans (to the benefit of foreign adversaries and their proxies), undermining a core goal for the Trump-Vance Administration.

As noted above, SEP abuses also represent one of the most glaring flaws in U.S. supply chains for critical and emerging technologies, presenting an economic and national security imperative. As a prime example, SEP licensing abuses are occurring in automotive supply chains where some SEP holders in foundational wireless communication standards refuse requests for FRAND licenses from reasonable and willing licensees. Instead they are arbitrarily insisting on licenses from the end product (the vehicle) in order to extract unrelated value beyond the components that function from the SEP, leaving suppliers in supply chains unable to get enough license for their components and indemnify their customers against SEP infringement claims. The net result has been to introduce preventable uncertainties and disruptions to these supply chains, undercutting important safety and sustainability goals, as well as U.S. economic and national security interests. Due to inaction by the Biden-Harris Administration, foreign adversaries and their proxies (such as state-controlled enterprises and strawman SEP pools) are well positioned to exploit and shut down U.S. supply chains.

Notably, courts in foreign markets are being wielded to solidify controlling roles in critical U.S. supply chains. SEP licensor abuse-driven disruptions to supply chains are being perpetuated by foreign courts, including in China, that have concluded that they can force a standards user to accept global FRAND terms on pain of a national injunction. The precedent set by such decisions has (1) emboldened Huawei to abuse their dominant market position in key telecommunication standards; and (2) encouraged other foreign SEP holders to similarly harm American economic and national security interests by excluding competitors and disrupting mature supply chains.

### ***Government-Backed Chinese Enterprise Huawei Deploys Strategic Efforts to Corner and Exploit the Market for SEPs in Connectivity Standards***

Founded in 1987, Huawei is a prominent company in the global telecommunications market for its sale of network equipment and devices, with demonstrated links to the Chinese government and military. Since 2000, Huawei's origins and behavior have given rise to serious national and economic security concerns for the U.S. government.<sup>8</sup> In 2019, the U.S. Department of

---

8

<https://crsreports.congress.gov/product/pdf/R/R47012/2#:~:text=For%20more%20than%20two%20decades,its%20expansion%20globally%2C%20and%20the>

Commerce added Huawei to its Entity List, a decision that effectively banned the company from buying parts and components from U.S. companies without U.S. government approval. As also noted by CRS, the first Trump Administration imposed, and the Biden Administration upheld, upheld Huawei-related restrictions and tightened restrictions on sales of semiconductors for 5G devices.

Already holding more than 22,000 granted patents in the United States, Huawei has positioned itself as prominent aggressor against U.S. companies, including leading American telecommunications company Verizon. Notably, Huawei has transferred 766 3GPP-related patent assets to a new non-practicing entity that is publicly noting its intent to target U.S. companies.<sup>9</sup> Huawei is a long-time abuser of the standards system by way of anticompetitive SEP licensing practices leveraged directly by the SEP holder or through patent pools. Huawei has demonstrated its willingness to target and pack critical standards like 5G (where it is the clear leading holder of SEPs), positioning itself to exert disproportionate control over significant industries that incorporate connectivity into products.

Huawei has been front and center for a many major international SEP disputes around the world, including the United States:

- **NETGEAR** was forced to sue Huawei in California federal court in response to Huawei's UPC suit under a civil Racketeer Influenced and Corrupt Organizations Act (RICO) claim for weaponizing their SEPs to obstruct U.S. the competitor from complying with international standards.
- Huawei has targeted **Tesla** in SEP lawsuits in the United Kingdom where it has sought to have the UK courts impose global terms (including for the United States) when only 7 percent of the relevant patents were UK patents.<sup>10</sup>
- Further, targeting the automotive industry, since 2022 Huawei has sued **Stellantis** automotive group (Fiat, Opel, Peugeot, and Citroën) in the German court system alleging SEP infringement, significantly disrupting automotive supply chains.<sup>11</sup> Auto manufacturer Continental has detailed the impacts of SEP abuses on the industry.<sup>12</sup>
- Huawei's established strategy includes weaponizing jurisdictions abroad where injunctions on SEPs can be improperly attained,<sup>13</sup> including Brazil where Huawei has already made 1794 patent applications since 2018.<sup>14</sup>
- In 2024, Huawei has utilized the Munich division of the EU's newly-established Uniform Patent Court (UPC) to pressure American companies **NETGEAR** and **Amazon** into excessive licensing fees. The Munich division is particularly attractive to opportunistic SEP holders like Huawei for its tendency to apply a German approach to SEP disputes with the power to award an injunction that applies across 18 EU Member States.<sup>15</sup>

The above examples are only what is known from public reporting, and Huawei's activities, enabled by a lack of U.S. policy leadership, reach far deeper and wider. They are not publicly disclosed, however, because of the high percentage of legal disputes that settle and because Huawei, like many other foreign SEP licensors, insist on overly-broad non-disclosure

---

<sup>9</sup> <https://www.iam-media.com/article/huawei-transfers-766-3gpp-related-patent-assets-new-npe>.

<sup>10</sup> <https://www.law360.co.uk/articles/2267824>.

<sup>11</sup> <https://www.lexology.com/library/detail.aspx?q=b6466f6d-b998-4e85-a96c-de3e06da7719>.

<sup>12</sup> <https://www.regulations.gov/comment/USTR-2023-0014-0040>.

<sup>13</sup> <https://www.iam-media.com/article/inside-huaweis-americas-ipr-department>.

<sup>14</sup> <https://www.iam-media.com/article/the-top-chinese-patent-holders-adding-brazil-their-strategic-maps>.

<sup>15</sup> <https://ipfray.com/new-huawei-v-netgear-filings-discovered-in-munich-and-upc-interim-conference-to-take-place-next-week-wifi-6-seps/>.

agreements that prohibit revealing their abuses. Further, in an effort to shield itself from SEP abuses, Huawei has committed thousands of its SEPs to Sisvel SEP patent pools for key technology areas including Wi-Fi, cellular IoT, and others. Sisvel, an EU-based patent pool operator, enables Huawei to separate itself from notorious SEP licensor abuses.

*Further background/critical information:*

- “From sanctions to success: Huawei’s novel strategy – IP licensing” <https://www.fierce-network.com/wireless/sanctions-success-huaweis-novel-strategy-ip-licensing>

***The Trump-Vance Administration Should Protect American Economic And National Security Interests Against Foreign Adversaries Like Huawei, Who Are Increasingly Abusing Their SEP Holder Positions To Exclude Competitors And Disrupt Key Supply Chains In Order to Further The Interests Of Foreign Adversaries***

The United States has the means to deter SEP-related threats to American economic and national security, and should take the following steps:

- **Setting clear Administration policy** that supports innovation and protect national security by reinforcing that:
  - FRAND-committed SEP licenses are to be made available to any licensee needing a license in order to implement a standard;
  - Prohibitive orders (injunctions from a district court and exclusion orders from the International Trade Commission) for FRAND-committed SEPs are to be awarded only in exceptional circumstances, such as when monetary remedies are not available;
  - FRAND royalties are to be based on the value of the patented technology itself;
  - FRAND-committed SEPs should respect the principle of patent territoriality;
  - The tying of non-essential patents in with FRAND-committed SEP licensing requirements is prohibited; and
  - The FRAND commitment follows the transfer of a SEP.
- **Uphold good case law**, such as the U.S. Supreme Court precedent, *eBay v. MercExchange*, which established a test to determine when an injunction is appropriate in a patent dispute. This precedent prevents bad faith patent holders, including non-practicing entities, from using the U.S. patent system to deplete U.S. innovation and harm downstream consumers.
- **Bolster key mechanisms that ensure patent quality**, including the Patent Trial and Appeal Board (PTAB) which allows U.S. entities to challenge vague, obvious and potentially invalid patents so that they cannot be frivolously enforced.
- **Increase antitrust enforcement** against Huawei and other opportunistic SEP holders to prevent foreign entities and their adversaries from holding technical standards hostage, harming American businesses and increasing costs for American consumers.
- **Leverage restrictions, sanctions, and tariffs** against foreign adversaries and their proxies who target American innovators and jeopardize U.S. supply chains through SEP abuses.

## *B. Copyright*

Copyrights protect original expressions of authorship, in physical form like literary or artistic works (books, music, sound recordings, movies, paintings) and digital forms like software, codes, and databases. Intentional theft or infringement of copyrighted materials, commonly known as piracy, presents existential risks and harms to U.S. small business digital economy innovators.

App Association members are both content creators and users. While software and creative content are a valuable part of an intellectual property portfolio, developers also license software and content for use in their own products and services. Software piracy jeopardizes the success of our members and threatens digital content creators' ability to innovate, invest, and hire. Even free, ad-supported applications have their content stolen and new ad networks embedded, making honest developers bear the cost of distributing content while not seeing a dime of ad revenue. Other free apps are pirated to create botnets and commit crimes where the use of the reputation of the legitimate developer lures unsuspecting victims. Like many other industries, the app industry experiences significant loss of revenue each year from piracy and counterfeits. Piracy threatens not only a developer's ability to innovate, invest, and hire but also threatens end-user confidence when consumers become victims of illegal distributors who pose as legitimate sellers. Counterfeit software apps can lead to customer data loss, interruption of service, device malfunction and data privacy risk.

Small software developers are also concerned about the increasing ubiquity that advanced AI systems have introduced around the copyright protection of software developed through both open- and closed-source models. Small business software developers' ability to create competitive products that integrate AI technology across markets is disproportionately harmed by this lack of clarity. Our members and software developers at large play a crucial role in shaping an innovation landscape where strong copyright protections align with the advancement of AI.

**To support U.S. small business growth and job creation through copyright policy, we urge the Trump-Vance Administration to:**

- **Increase law enforcement activities against copyright pirates, and work with other governments to accomplish the same;**
- **Rapidly put an Intellectual Property Enforcement Coordinator (IPEC) in place in the White House.**



### *C. Trademark*

Trademarks protect distinctive signs, symbols, words, names, devices, colors, and more that identify and distinguish one's products or services from the products or services of others. Our members allocate time and resources in developing their business brand, and protection of their logo is integral to building and protecting their reputation.

Trademarks are an essential part of branding and are key to building trust with customers. As cutting-edge creators, our members rely on trademarks to conduct their business every day. Unfortunately, bad actors want to appropriate the success of our members' businesses through brand confusion. The App Association works with our members to advance their understanding of trademark rights and to encourage their trademark registration before a problem arises.

**To support U.S. small business growth and job creation through trademark policy, we urge the Trump-Vance Administration to:**

- **Rapidly put an Intellectual Property Enforcement Coordinator (IPEC) in place in the White House;**
- **Support small business efforts to enforce against trademark infringements, and work with other governments to accomplish the same.**

### *D. Trade Secrets*

Trade secrets encompass information, like a formula, program device, method, or technique that: (i) derives independent economic value from being generally unknown and not readily ascertainable by proper means and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Examples of trade secrets include blueprints, customer lists, pricing information, and source code.

Our members also rely on trade secrets, or practices used by businesses that allow them to maintain a competitive advantage. In particular, trade secrets are essential for software that uses machine learning or artificial (or augmented) intelligence. As the Administration considers transparency requirements for such algorithms, they should be mindful that trade secrets are integral to the software developer business model, and without trade secrets, the incentive to create is lost.

**To support U.S. small business growth and job creation, we urge the Trump-Vance Administration to:**

- **Increase law enforcement activities against theft of trade secrets, and work with other governments to accomplish the same;**
- **Rapidly put an Intellectual Property Enforcement Coordinator (IPEC) in place in the White House.**

## **Broadband and Telecommunications**

Too many Americans do not have adequate access to high-speed mobile broadband internet, leaving them on the wrong side of the growing digital divide. To reach these underserved and unserved Americans across the country, the federal government must incent and support the deployment of needed infrastructure.

Now more than ever, Americans depend on the internet to communicate, get jobs, access healthcare services, go to school, and otherwise participate in society. Therefore, the future of the app economy depends on the strength and density of America's broadband networks. The deployment of next generation wireless networks will enable improvements in economic productivity, employment, and consumer value. 5G and successor technologies will affect the labor market through direct and indirect means, with the broadest impact coming from jobs enabling new applications, services, ways of doing business, and general growth of businesses.

Without accurate maps, informed decisions on broadband policy cannot occur. The App Association supports federal efforts to connect Americans to high-speed internet through improved broadband maps, which will drive better access to broadband. More accurate and granular maps that can correctly identify unconnected and underserved communities and areas are essential to a variety of federal programs and efforts and would assist App Association members in product development.

Across the country, App Association small business innovator members rely on high-capacity wireless broadband networks to compete across sectors of the economy. Federal policymakers must take steps to address numerous well-documented barriers that unnecessarily add costs and time to broadband infrastructure deployments through means such as "shot clocks" for small cell applications and "dig once" infrastructure funding policies.

Further, to address last-mile connectivity challenges, federal policymakers must support spectrum allocations that enable 5G innovations in America by opening more bands to both licensed and unlicensed uses, including through dynamic sharing arrangements, based on sound engineering analyses.

**The Trump-Vance Administration can support U.S. small business growth and job creation through its broadband and telecommunications policies by:**

- **Prioritizing the development of publicly accessible broadband maps with improved depth and accuracy;**
- **Streamlining broadband infrastructure buildouts, and encouraging Congressional oversight to achieve this goal;**
- **Supporting a staggered reallocation and/or sharing of certain spectrum bands identified as ideal for use by next-generation connectivity and innovations—a "spectrum pipeline"—to support America's goals and create jobs.**

## Cybersecurity

App Association members share the Trump-Vance Administration view that the protection of personal and sensitive information is vital to U.S. economic and national security. That holds especially true when the personal information at issue involves the contents of users' private communications or other sensitive information.

With the frequency and complexity of cyber-based attacks continuously increasing, small businesses in the digital economy are at the most risk because they have far more limited resources than large companies. Up to 71 percent of cyberattack targets are small companies, which suffer disproportionately from successful breaches. The average cost of a breach is now around \$653,587 for small businesses, which can destroy the firm. And the most sophisticated attacks routinely originate with foreign adversaries, either directly or through proxies. Even further, the shortage of cybersecurity professionals in the American workforce exacerbates challenges with attack detection, prevention, and mitigation.

App Association small business members, who typically do not have multiple product lines to distribute organizational risk across, are dedicated to security by design and security by default but need support and assistance in the integration of security measures while maintaining a competitive speed to market. Indeed, security by design is a priority driven by the market today as much as compliance with laws and regulations, which is why our community goes far above and beyond legal requirements to proactively ensure security from the earliest phases of design and development.

Maintaining a nimble and responsive cybersecurity risk management posture requires leveraging the best tools available, namely strong encryption. Proposals to undermine encryption—for example, through mandated backdoors to an algorithm or by requiring the scanning of user communications for surveillance purposes—cannot coexist with the ability to use encryption to support trust and security. As a prime example, the [Salt Typhoon attacks](#) in late 2024—which took advantage of mandatory backdoor access for law enforcement built into broadband networks—illustrate that backdoors necessarily lead to compromise.

Along with the National Institute of Standards and Technology (NIST), the Department of Homeland Security's Cybersecurity and Information Security Administration (CISA) should serve as a leader and coordinator within the U.S. government in guiding the management of cybersecurity risk across sectors, supporting sector-specific agency activities where needed. We appreciate that CISA, like NIST, embraces a scalable cybersecurity risk management approach that enables developers to adjust their cybersecurity risk management tactics to anticipated harms/intended uses and the unique circumstances in play for that product or deployment. It is vital that this approach be maintained.

**The Trump-Vance Administration should pursue the following priorities to support American cybersecurity:**

- **Building on the NIST Cybersecurity Framework, take a risk-based approach to cybersecurity requirements in alignment with standardized approaches to risk management, including through harmonizing requirements across domestic policymakers (NIST, FedRAMP, etc.);**
- **Provide further support for small businesses in the digital economy that will increase their ability to detect and mitigate cybersecurity vulnerabilities, including by supporting and rewarding security-by-design practices;**

- **Lead in providing liability protections for small businesses that experience cybersecurity attacks and react with good faith, reasonable steps, including in sharing timely incident information with the government;**
- **Support the use of technical protection mechanisms, including encryption, to provide for end user trust, opposing calls for mandated backdoors to encryption; and**
- **Work with Congress to provide resources for educational efforts and training that will help address the national cybersecurity workforce shortage.**

## **Privacy**

Protection of consumers' data and trust is of the utmost importance to the small business community the App Association represents. Now more than ever, small businesses and startup innovators rely on a competitive, trustworthy, and secure ecosystem to reach millions of potential users across consumer and enterprise opportunities so they can grow their businesses and create new jobs.

Small businesses go far above and beyond minimum legal requirements. Today, privacy protection is a means of market differentiation, and we caution the Trump-Vance Administration (and Congress) from altering this digital economy dynamic. Further, we urge that the incoming Administration ensure that its claims of harms are based on a strong and data-driven evidence base, and that its policy actions are not driven by rare edge use cases and/or hypotheticals.

The App Association is committed to a unified national policy that provides the small business community with a privacy framework to protect consumers. Ultimately, the App Association agrees that the time for changes to the U.S. approach to privacy regulation (a growing number of sector-and state-specific approaches) has arrived. The App Association is supportive of a new federal privacy framework that will clarify the obligations of our members and pre-empts the fractured state-by-state privacy compliance environment, and generally urges that the U.S. approach to privacy provide robust privacy protections that correspond to Americans' expectations, as well as leverage competition and innovation. With numerous state-level comprehensive privacy frameworks in place, the European Union's General Data Protection Regulation (GDPR), and a host of other regulatory regimes in various stages of consideration and implementation, it is likely that the 119th Congress will consider some form federal privacy legislation. For small businesses, the twin imperatives for privacy rules are to provide regulatory clarity and to avoid taking away the tools they use now. The App Association therefore recommends that federal agencies, including the FTC, stand back on new rules and instead provide guidance per their existing authority on consumer privacy while Congress' work on new legislation continues.

A federal law more intentionally focused on curbing privacy harms should empower consumers to exert more control over their sensitive personal information, including the rights to access, correction, and deletion of such information. Sensitive personal information should also be subject to some flexible limits on processing activities that pose too great a risk to consumers. Unlocking the innovative potential for life-saving technologies requires the establishment of a single set of strong, national privacy requirements based on a clear delegation from Congress.

**The Trump-Vance Administration can take immediate steps to improve Americans' privacy throughout their lives by:**

- **Supporting legislation to create a federal data privacy framework with strong preemption of state laws, a path to compliance for small businesses, and enforcement focused on specific harms so as not to stifle innovation;**
- **Ensuring that online platforms continue to have the tools they need to protect the privacy and security of their customers; and**
- **Pushing back in the digital trade arena against other countries' policies that have the effect of reducing the privacy and security of Americans and their data.**

### **Trade and Market Access Abroad**

In a shocking and damaging move, the Biden-Harris Administration unilaterally withdrew its support for long-held U.S. positions on digital trade that have fostered the growth of the American small business digital economy. Notably, the Biden-Harris Administration's U.S. Trade Representative (USTR) withdrew these positions without consulting with Congress or other federal agencies, prompting strongly-worded statements opposing USTR's unconsidered abandonment of digital trade priorities came from both Republican<sup>16</sup> and Democratic<sup>17</sup> leadership of the committees with jurisdiction over trade. We also led a sign-on letter with several small businesses and organizations representing small businesses to the President urging his Administration to reconsider the decision.<sup>18</sup>

The pressure campaign leading to these decisions claims to seek policy changes to make larger technology companies more accountable, even though ample measures and processes under existing domestic laws exist to address concerns. This is especially ironic because it is pursuing a mechanism to achieve its goals by placing the future of American tech-driven industries in the hands of governments, like China, that are still at the negotiating table and that are decidedly *not* accountable to Americans. Further, USTR's withdrawal signals to our adversaries that we no longer will stand to preserve basic digital trade protections small U.S. companies rely on more heavily than larger counterparts, like the United States' previously unwavering opposition to data localization and source code inspection/escrow requirements as conditions of market entry. The Trump-Vance Administration's leadership is sorely needed to fix U.S. trade policy so that it advances U.S. economic interests by enabling American firms to compete in markets abroad on fair terms, a goal that is as much pro-business as it is pro-labor.

---

<sup>16</sup> "Chairman Smith Statement on Biden-Harris Administration's Decision to Surrender to China on Digital Trade Rules," press release, House Committee on Ways and Means (Oct. 26, 2023), *available at* <https://waysandmeans.house.gov/chairman-smith-statement-on-Biden-Harris-administrations-decision-to-surrender-to-china-on-digital-trade-rules/>.

<sup>17</sup> "Wyden Statement on Ambassador Tai's Decision to Abandon Digital Trade Leadership to China at WTO," (Oct. 25, 2023), *available at* <https://www.finance.senate.gov/chairmans-news/wyden-statement-on-ambassador-tais-decision-to-abandon-digital-trade-leadership-to-china-at-wto>.

<sup>18</sup> Letter from several small business organizations and small businesses to President Joseph R. Biden-Harris, Re: The Imperative for U.S. Government Support of Startups, Small Businesses, and Entrepreneurs in the Global Digital Economy, (Nov. 3, 2023), *available at* <https://actonline.org/wp-content/uploads/Small-Business-Ltr-re-USTR-Digital-Trade-3-Nov-2023-w-cosigners-1.pdf>.

**The Trump-Vance Administration should take immediate steps to advance U.S. trade policies that support American small businesses by:**

- **Supporting American small business access to new markets and customers by preserving cross-border data flows and preventing data localization requirements, including through new international data agreements;**
- **Prohibiting and fighting against customs duties and taxes on digital content;**
- **Prohibiting and fighting against foreign markets' mandating technology transfers/requiring source code escrowing/inspection as a condition of market entry;**
- **Documenting and confronting IP-related trade barriers, including a lack of enforcement, across developed and developing markets that small businesses operate in;**
- **Preserving the ability of American small businesses to leverage technical protection mechanisms, including encryption, as they operate in foreign markets;**
- **Opposing the discriminatory application of antitrust and consumer protection laws by foreign markets that aim to exclude U.S. companies from competing in their markets, and formally recognize such efforts as significant trade barriers.**
- **Reducing or eliminating tariffs on information and communication technology (ICT) goods that American consumers rely on to access small business innovations;**
- **Reducing regulatory confusion/overlap and advancing compliance complexity in new export controls; and**
- **Partnering with allies to advance trusted supply chains that will securely support the U.S. economy.**

## **Standards**

Consensus-based technological standards fuel innovation. Trusted standards-setting organizations (SSOs) convene stakeholders from around the ecosystem to develop these standards, which promote interoperability between products and services and address end user safety. Because standards have this role as a baseline to innovation, small businesses often need to utilize them to compete in the market. That said, standardization is not always the optimal path and sometimes the market naturally produces privately owned vertical stacks that serve competitors and consumers better than voluntary standards. Thus, technical standardization is always best understood as a voluntary enterprise. However, where standards are naturally the best option for interoperability, they level the playing field, opening opportunities to compete.

To advance American interests on the global stage, the United States must engage inclusively in international standards development. As foreign actors like China expand their influence in standards organizations, policymakers face pressure to assert national interests unilaterally or restrict participation. However, policies that foster consensus-driven, private sector-led approaches offer a better path for sustained U.S. leadership in AI.

We encourage the new Administration to support NIST's core functions while reinforcing in clear terms that NIST's role is not regulatory. Chronic underfunding has already impaired NIST's ability to meet its most important obligations, such as validating cryptographic modules and maintaining a robust Vulnerability Database. These functions are essential to ensure American technology makers can remain competitive in the global marketplace.

**To support American economic growth and leadership, the Trump-Vance Administration should:**

- **Protect NIST's core mission by keeping NIST focused on its technical advisory role in standards development, steering clear of regulatory overreach;**
- **Support open, private sector-led standards processes that enable the United States to lead globally while engaging constructively with international partners;**
- **Avoid policies that exclude specific entities or impose unilateral U.S. interests in global standards bodies, which could undercut long-term American leadership;**
- **Boost U.S. engagement in international standards organizations to ensure a strategic, collaborative presence; and**
- **Push for risk-based, quality-focused frameworks that prioritize safety and inclusivity, ensuring small businesses can innovate without excessive barriers.**