March 4, 2025

Robert Burkett
Acting Under Secretary of Commerce for Industry and Security
Bureau of Industry and Security
1401 Constitution Avenue Northwest
Washington, District of Columbia 20230

RE: Comments of ACT | The App Association, Bureau of Industry and Security Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems [Docket No. 241213-0327]

Dear Mr. Burkett:

ACT | The App Association (App Association) writes in response to the Department of Commerce's (DOC's) Bureau of Industry and Security (BIS) request for comments on its advance notice of proposed rulemaking (ANPRM) on issues related to transactions involving information and communications technology and services (ICTS) that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries that are integral to unmanned aircraft systems (UAS).[1]

I. Introduction and Statement of Interest

The App Association is a global policy trade association for the small business technology developer community. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. 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. App developers like our members also play a critical role in developing UAS innovations throughout ICTS UAS supply chains. 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.[2]

II. UAS are Part of a Broader Digital Ecosystem of Applications and Services

The App Association appreciates BIS' request for input on the ICTS supply chain for UAS in the United States, and shares the goal of realizing strong, sustainable, and secure ICTS supply chains across sectors. App Association members develop software and connected hardware at key points throughout ICTS UAS supply chains. UAS leverage GPS, radar, photos, and other

[1] 89 FR 15066.
[2] ACT | The App Association, State of the App Economy (2022), https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL.pdf.

data points securely and appropriately collected, which App Association members often leverage to innovate and compete.

As BIS considers new rules for the security of the ICTS supply chain, the App Association urges consideration of the reality that UAS are a part of the broader digital economy. Many UAS in the market today have access to and make use of third-party applications and services, and this will only increase as the digital ecosystem around UAS develops. BIS should be mindful that, while focused on security, its rules could amount to harmful digital trade barriers if not drafted with appropriate scope.

The small business innovators we represent prioritize the following general principles for policies affecting the international digital economy:

- ***Enabling Cross-Border Data Flows:*** The seamless flow of data between economies and across political borders is essential to the functioning of the global economy. Small business technology developers must be able to rely on unfettered data flows as they seek access to new markets.
- ***Avoiding Data Localization Policies:*** American companies looking to expand into new markets often face regulations that force them and other foreign providers to build and/or use local infrastructure in the country. Data localization requirements seriously hinder imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification. Our members do not have the resources to build or maintain unique infrastructure in every country in which they do business, and these requirements effectively exclude them from commerce.
- ***Prohibiting Customs Duties and Digital Service Taxes on Digital Content:*** American app developers and technology companies must take advantage of the internet's global nature to reach the 95 percent of customers who live outside of the United States. However, the tolling of data crossing political borders with the purpose of collecting customs duties directly contributes to the balkanization of the internet. These practices jeopardize the efficiency of the internet and effectively block innovative products and services from market entry.
- ***Ensuring Market Entry is Not Contingent on Source Code Transfer or Inspection:*** Some governments have proposed policies that require companies to transfer, or provide access to, proprietary source code as a requirement for legal market entry. Intellectual property is the lifeblood of app developers' and tech companies' innovation; the transfer of source code presents an untenable risk of theft and piracy. Government policies that pose these requirements are serious disincentives to international trade and a non-starter for the App Association's members.
- ***Preserving the Ability to Utilize Strong Encryption Techniques to Protect End User Security and Privacy:*** Global digital trade depends on the use of strong encryption techniques to keep users safe from harms like identity theft. However, some governments continue to demand that backdoors be built into encryption keys for the purpose of government access. These policies jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a privacy and security standpoint, the viability of an app company's product depends on the trust of its end users.
- ***Securing Intellectual Property Protections:*** The infringement and theft of intellectual property and trade secrets threatens the success of the App Association's members and

hurts the billions of consumers who rely on these app-based digital products and services. These intellectual property violations can lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone a potential "end-of-life" occurrence for a small app development company. The adequate and effective protection and enforcement of intellectual property rights is critical to the digital economy innovation and growth.

- ***Avoiding the Misapplication of Competition Laws to New and Emerging Technology Markets:*** Various regulators, including key trading partners, are currently considering or implementing policies that jeopardize the functionality of mobile operating systems and software distribution platforms that have enabled countless American small businesses to grow. Since its inception, the app economy has successfully operated under an agency-sale relationship that has yielded lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections for app developers with little-to-no government influence. Foreign governments regulating digital platforms inconsistent with U.S. law will upend this harmonious relationship enjoyed by small-business app developers and mobile platforms, undermine consumer privacy, and ultimately serve as significant trade barriers.

III. BIS ICTS Rules Should Adopt Clear and Targeted Definitions

The App Association encourages BIS to resolve vague definitions for UAS, which would, if advanced as drafted, include all segments of the UAS industry. We urge BIS to clearly and specifically define UAS classes/supply chains that it seeks to apply ICTS rules to in order to provide clarity to the industry about impacted products, providing key use cases as guidance/to advance understanding.

IV. BIS ICTS Rules Should Avoid Data Localization Requirements

As discussed above, data and processing localization requirements ignore the efficiencies and security of distributed cloud computing and do not translate to assurances of data security, instead creating unnecessary barriers to trade and innovation. The App Association strongly urges BIS to avoid local data storage or processing mandates in its rules. Such a requirement would be inconsistent with UAS industry leading standards for data collection and processing.

V. BIS ICTS Rules Should Preserve the Ability to Secure Data and Supply Chains Using Encryption

Whether as a contractor or as a business partner, App Association members are required to share sensitive information with developers of UAS in the normal course of business using cloud computing services. They rely on risk management best practices and technical protection mechanisms to securely accomplish these vital interactions, which may include remote access and/or providing firmware or software updates. As it advances rules for ICTS UAS, BIS should maintain the ability to leverage these technical protection mechanisms such as encryption, without which the secure data flows that underpin secure supply chains could not exist.

VI. BIS ICTS UAS Rules Should Align with Leading Risk Management Practices

The App Association also urges BIS to align with leading federal guidance from the National Institute of Standards and Technology (NIST) on cybersecurity and supply chain risk management[3] as well as sector-specific guidance from the National Highway Traffic Safety Administration (NHTSA),[4] when crafting its regulations, which enable the scaling of risk mitigation practices to the harms presented. Such an alignment will ensure that BIS rules enable the industry to most efficiently identify, assess, and mitigate the risks associated with the distributed and interconnected nature of ICTS UAS supply chains across the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction).

VII. Technology Standardization Has a Crucial Role in Supporting Secure and Strong ICTS Supply Chains For UAS

A. Historical Abuses in Standard-Essential Patent Licensing Have Reached UAS

Technology standards provide the foundation for many ICTS-based inventions that make UAS "smart." Technical standards provide an efficient and interoperable base for technology developers to create new inventions that increase the quality, safety, and reliability of UAS for consumers and businesses alike. These standards are subject to a larger standard-setting process housed by standard-setting organizations (SSOs) that facilitate the open and consensus-based development of a standard and guide the equitable and reasonable implementation of the standard. When a patent holder contributes their technology to a technical standard, they provide SSOs with a commitment that they will license their so-called standard-essential patents (SEPs) on fair, reasonable, and non-discriminatory (FRAND) terms in exchange for access to a wider pool of licensees. Therefore, by contributing to the standardization process, a SEP holder consents not to unduly exclude competitors from a standard past requiring a FRAND SEP license.

Unfortunately, there are well-documented SEP licensing abuses that disrupt mature and crucial supply chains, including for UAS. Longstanding evidence shows that a minority of well-resourced and opportunistic SEP holders, including non-practicing entities (NPEs), abuse their monopoly positions by discarding the FRAND commitments they have made to attain unreasonable terms and excessive royalty rates. Since SSOs facilitate access to technical standards that touch various industries, these opportunistic SEP holders plague many verticals, always looking for the next market to extract additional and unrelated value for their SEP. The anticompetitive harms experienced in the SEP licensing ecosystem disrupt fair access to technical standards that support efficient innovation.

These SEP holders routinely refuse to license to certain upstream entities in the supply chain, while instead licensing to downstream entities, such as end product manufacturers, from whom they can extract additional value for a SEP holder's patented technology from unrelated features of the implementing product. The practice by SEP holders to extract value from components of

[3] E.g., https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.
[4] https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-UAS-2022-tag.pdf.

the implementing technology that do not function based on the SEP has been discouraged on a global scale.[5] This evidence is at odds with the position held by certain patent pools that claim they are not beholden to the FRAND commitment attached to the SEPs they license, which causes significant uncertainty in supply chains.[6]

The UAS sector's supply chains are vulnerable to SEP licensing abuses. Opportunistic SEP holders that have patents covering wireless communication standards often choose what manufacturer in the UAS supply chain to license their SEP to, causing uncertainties about indemnification for other manufacturers. The same SEP holders seek licensing fees that extract value out of the end product (the UAS) beyond the components that function from the SEP. This process slows down innovation in UAS that are geared toward achieving important safety and sustainability goals.

B. Foreign Jurisdictions That Support Standard-Essential Patent Licensing Abuses Amplify Harm to U.S. Innovation

Numerous intellectual property rights (IPR) policies of SSOs and foreign jurisdictions threaten both U.S. leadership and participation in international standard setting, and the growth of U.S. innovators that rely on the ability to readily license SEPs. A trend of court decisions abroad, starting in the United Kingdom (UK)[7] and European Union (EU),[8] have distorted the meaning of the FRAND commitment, creating an imbalance that heavily favors SEP holders by routinely enabling prohibitive orders (injunctions) for FRAND-committed SEPs. For example, Germany's approach to SEP injunctions has caused immense disruptions to supply chains across several industries and has resulted in various companies ceasing operation in the country because of the inability to reliably use standards (due to an imbalanced approach to SEP injunctions), fraying the international norm for limited inunctions on FRAND-committed SEPs and undermining international standards.

These decisions have enabled (and emboldened) SEP holders to systematically abuse their dominant market position as a gatekeeper to the use of the standard to attain supra-FRAND terms (a practice known as hold-up).[9] Some foreign courts have concluded that they can force a standards user to agree to a global SEP portfolio on FRAND terms set by the court or SEP holder on pain of a national injunction if the standards user does not agree to the license. In such decisions, the global SEP licenses at issue often include patents issued outside the court's jurisdiction for which validity and essentiality have not been assessed. The precedent set by such decisions has done two things to the landscape of international standards: (1) allowed

---

[5] Interdigital Technology Co. v. Lenovo Group Ltd. [2023] EWHC 126, 539 (Pat). Para 247 ("When a mobile phone, tablet or computer uses 3G, 4G or 5G technology covered by SEPs, the royalties payable should not depend on the price of the phone (or tablet or computer), which reflects many other features (e.g. screen size, processor power and other features) which are unrelated to the licensed technology even if dependent on it, as well as the status of the brand of phone or tablet.").
[6] *See* Continental Automotive Systems v. Avanci, LLC, No. 20-11032 (5th Cir. 2022).
[7] See *Unwired Planet International Ltd v. Huawei Technologies Co. Ltd* (SCUK 2020).
[8] *See* Sisvel v Haier, Federal Court of Justice, judgment dated 5 May 2020, Case No. KZR 36/17; *see* Koninklijke Philips N.V. v. Wiko SAS, Court of Appeal of The Hague, judgement dated 2 July 2019, Case No. C/09/511922/HA ZA 16-623.
[9] Lemley, Mark A. and Shapiro, Carl, Patent Holdup and Royalty Stacking. 85 Texas Law Review 1991 (2007).

jurisdictions to exercise extrajudicial authority on patents outside their purview;[10] and (2) encouraged certain SEP holders to forum shop to a more favorable jurisdiction to handle the outcome of their disputes when they are unable to force implementing standards users into unreasonable licensing terms, despite their FRAND obligation.

C. BIS Should Address Standard-Essential Patent Licensing Issues That Disrupt Supply Chains in UAS

The App Association urges BIS to ensure that its ICTS transaction rules support U.S. UAS supply chain security and resiliency. In addressing ICTS transactions for UAS, BIS should recognized and prevent bottlenecks in SEP licensing that are barriers to trade and which threaten the resilience of U.S. supply chains, namely those SEP licensor hold-up practices that have been well demonstrated with empirical evidence.[11] If U.S. manufacturers are unable to reliably develop critical components that affect consumer safety and privacy and the quality of U.S.-made UAS without fear of potential and likely lawsuits from opportunistic SEP holders, many inventors will forgo production. The DOC can address these issues by increasing transparency in the FRAND SEP licensing process through a public database for base level SEP information, a government-led SEP Policy Statement, and support in U.S. participation in international standards.

BIS should, in coordination with others including the United States Patent and Trademark Office (USPTO), to secure UAS supply chains. As one example, BIS ICTS transaction requirements should contribute to providing a base level of information that a SEP licensor provides to licensees outside overly restrictive non-disclosure agreements (NDAs) that hide comparable licensing rates and terms. BIS' efforts to provide more transparency in FRAND licensing disputes through public databases would assist in facilitating fair negotiations between two licensing parties without significant intervention. We consider the following information to be "base level:"

- Information (e.g., patent list) to enable a licensee and entities within its supply chain to understand the SEPs being enforced;
- Detailed specification (e.g., claim charts) on the nature of the patent's alleged infringement by the licensee's technology, and ancillary information necessary for the licensee to assess claims of infringement, validity, and essentiality;
- FRAND licensing terms;
- Aspects of prior licensing history and any other information are needed to evaluate to offered and potential FRAND terms.

BIS should equally promote a balance between a SEP holder's patent rights and reasonable access to technical standards for those needing licenses in order to use standards and secure their supply chains by supporting broadly-accepted principles reflecting the meaning of the FRAND commitment. A balanced and pro-innovation multi-agency policy statement that

---

[10] Bonadio, Enrico, Mohnot, Rishabh, Standard Essential Patents, Global Licensing Approach and the Principle of Territoriality (September 6, 2022), https://patentblog.kluweriplaw.com/2022/09/06/standard-essential-patents-global- licensing-approach-and-the-principle-of-territoriality/.

[11] See Love, Brian J. and Lefouili, Yassine and Helmers, Christian, Do Standard-Essential Patent Owners Behave Opportunistically? Evidence from U.S. District Court Dockets (November 8, 2020). Available at SSRN: https://ssrn.com/abstract=3727085.

presents a whole of government approach to mitigating harmful SEP licensing abuses is key to amicable resolutions to FRAND licensing disputes. Policy solutions that facilitate more transparency in the licensing process can provide licensing parties with reasonable information to conclude a FRAND SEP license. These procedures are more crucial for entities that lack the professional and financial resources as their larger competitors, like small and medium-sized businesses. These policy solutions also provide courts and tribunals with evidence compiled through an expert opinion. These opinions should not prevent the court or tribunal from making an independent determination.

An important component of securing and strengthening supply chains is supporting U.S stakeholder participation in international technology standards development around ICTS innovations. The IP-based incentives in the standardization process differ from non-essential IP incentives. Patents are contributed to the standardization process to enable more inventors to use that standard. In this process, SEP holders are owed reasonable royalties for the use of their patented invention. The United States Government National Standards Strategy on Critical and Emerging Technology (USG NSSCET) is clear that the success of the voluntary, consensus-based, open-participation technology standards system is vital for U.S. competitiveness and national security. The success of this system to standards development is that industry participants are providing competing patent contributions and approaches. This system enables the market to determine a company's success and incents standardized technology development. This system ensures that internationally adopted standards are high quality, incorporate U.S. stakeholder input, and benefit all standards users. The consensus-based, open-participation technology standards system must be preserved in order to protect competitive standards that include U.S. leadership and involvement. Therefore, BIS should work with NIST to support U.S. participation and leadership in international technical standards.

We further urge BIS to consider the App Association's detailed views on SEP abuses and their harmful impacts on U.S. supply chains across CETs, which are appended to this comment.[12]

[12] Appendix A.

VIII. Conclusion

The App Association appreciates the opportunity to provide comments to BIS on securing the ICTS UAS supply chains.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

Priya Nair
Senior IP Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

Memorandum

Date: December 10, 2024

To: President-Elect Donald Trump
Policy Advisor

From: ACT | The App Association

Re: Promoting a Competitive Standard-Essential Patent Landscape

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) solutions while impacting a broad range of 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 patent holders choose to contribute their technologies to a technical standard, they understand and agree that their patents may be needed 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.

The App Association maintains that the following principles underlay a universal understanding of the FRAND commitment:

1. **The FRAND Commitment means all can license –** A holder of a FRAND-committed SEP must license that SEP to all companies, organizations, and individuals who use or wish to use the standard on FRAND terms.

2. **Prohibitive orders on FRAND-committed SEPs should only be allowed in Rare circumstances –** Prohibitive orders (including federal district court injunctions and U.S. International Trade Commission exclusion orders) should not be sought by SEP holders or allowed for FRAND-committed SEPs except in rare circumstances where monetary remedies are not available.

3. **FRAND royalties –** A reasonable rate for a valid, infringed, and enforceable FRAND-committed SEP should be based on the value of the actual patented invention itself to the smallest saleable patent practicing unit, which is separate from purported value due to that patent's inclusion in the standard, hypothetical downstream uses, or other factors unrelated to invention’s value.

4. **FRAND-committed SEPs should respect patent territoriality** – Patents are creatures of national law, and courts should respect the jurisdiction of foreign patent laws to avoid overreach with respect to SEP remedies. Absent agreement by both parties, no court should impose global licensing terms on pain of a national injunction.

5. **The FRAND commitment prohibits harmful tying practices –** While some licensees may wish to get broader licenses, a SEP holder that has made a FRAND commitment cannot require licensees to take or grant licenses to other patents not essential to the standard, invalid, unenforceable, and/or not infringed.

6. **The FRAND commitment follows the transfer of a SEP –** As many jurisdictions have recognized, if a FRAND-committed SEP is transferred, the FRAND commitments follow the SEP in that and all subsequent transfers.

I. *SEP Licensing Abuse Is Harming The United States' Leading Patent System*

The United States has the leading global patent system due to its strong emphasis on developing mechanisms that support innovation and foster competition and technological progress. Technical standards provide an alternative path to modern invention that differs from general exclusive patenting. The goal of establishing technical standards is to create an efficient and interoperable foundation for technology development that can be used by any industry participant who is willing and able to fairly compensate the relevant SEP holder. The SEP holder understands and agrees that, by contributing to the standardization process, it cannot unduly exclude competitors from a standard past requiring a FRAND license.

Opportunistic SEP holders have distorted this system by taking advantage of SSO policies that have ambiguous definitions of FRAND to manipulate a fair licensing negotiation process by, for example, overcharging or refusing to license to certain entities in a supply chain. Since SSOs facilitate access to technical standards that touch various industries, these opportunistic SEP holders plague many verticals, always looking for the next market to extract additional and unrelated value for their SEP. The anticompetitive harms experienced in the SEP licensing ecosystem disrupt fair usage of technical standards that support efficient innovation.

II. *Foreign Companies Use Their SEPs Against U.S. Companies*

It has become increasingly evident that foreign SEP holders are able to harm U.S. businesses and U.S. consumers through SEP licensing disputes, extracting billions of dollars out of the U.S. economy. Companies such as Huawei, Nokia, Ericsson, and Abu Dhabi-backed Fortress Investment Group continue to use the U.S. International Trade Commission (ITC) and foreign courts against U.S. businesses that are locked-in to key technical standards (e.g., 5G and Wi-Fi).

The ITC provides foreign entities that hold U.S. patents with the opportunity to bypass equitable tests in U.S. courts that determine if an injunction is appropriate by providing an exclusion order as the sole remedy. Ericsson and Nokia are avid users of the ITC to initiate SEP disputes against American companies, including Amazon and Apple. Similarly, these entities have used foreign courts, including the newly established Unified Patent Court (UPC), to seek injunctions and apply pressure to U.S. companies that are willing to conclude a FRAND-encumbered SEP license.

Some of these foreign companies stack their SEPs for key technical standards in foreign patent

pools that shield its members from individual FRAND obligations and disincentivize its members from licensing outside the highly inflated pool royalty rate. For example, Huawei holds a majority of the SEPs covering the 5G standard, which are licensed through the patent pool, Sisvel. This pool often uses German courts, known to award injunctions prior to determining a patents' validity, to litigate their SEP disputes. These decisions have enabled (and emboldened) foreign SEP holders to systematically abuse their dominant market position as a gatekeeper to the use of the standard to attain supra-FRAND terms (a practice known as "hold-up" [1]).

Where hold-up practices are stronger, U.S. inventors have less of an incentive to invest significant resources into patentable developments that are likely to be targeted by monetization schemes enforcing older, broader, and potentially invalid patents. While the U.S. patent landscape includes important mechanisms to combat issuing expansive patent claims and enables entities to challenge such patents post-issuance, many overly broad patents still exist and are ripe for abuse.[2] One recent example of this was revealed in a case between the State of Washington and "patent troll" Landmark Technology A, where internal litigation communications revealed bad faith licensing tactics, such as the targeting of nearly 1,200 different companies across 18 months using an extremely broad and likely enforceable patent, demanding $65,000 in licenses fees.[3] Even without a credible threat of an injunction, many of the targeted small companies across diverse industries ultimately settled to avoid costly litigation fees.[4]

SEP licensing abuse is often supported by third-party litigation funding (TPLF), a mechanism used to abuse patent process in the United States and internationally against U.S. companies. Non-practicing entities (NPEs) initiate a majority of the abusive and frivolous patent infringement suits in the United States[5] and many NPE suits are financially backed by unnamed investors hidden through shell corporations or wealth funds that may have a real interest in the outcome of litigation.[6] TPLF has affected critical U.S. technology industries, including telecommunication, automotives, and semiconductors. Funders may be individual entities seeking economic gain or competing countries strategically undermining essential U.S. industries and U.S. national security. The availability of anonymous investment sources enables bad actors to flood adjudicating bodies with potentially illegitimate claims. Abu Dhabi-back Fortress Investment Group has been identified numerous times as an undisclosed funder of patent holders initiating frivolous disputes in the United States.[7]

---

[1] Lemley, Mark A. and Shapiro, Carl, Patent Holdup and Royalty Stacking. 85 Texas Law Review 1991 (2007).
[2] *See* 35 U.S.C. 101; *see* Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat.(2011).
[3] *See* Declaration, *State of Washington v. Landmark Technology A LLC*, NO. 2:21-cv-00728-RSM (W.D. Wash 2022), ECF No. 97; *see also* Dani Kass, Law360, *Wash. Urges Federal Court To Set Bad Faith Test For IP Cases* (April 23, 2024), https://www.law360.com/articles/1827562/wash-urges-federal-court-to-set-bad-faith-test-for-ip-cases.
[4] Office of the Attorney General of Washington, *AG Ferguson files lawsuit against "patent troll" targeting small businesses* (May 14, 2021), https://www.atg.wa.gov/news/news-releases/ag-ferguson-files-lawsuit-against-patent-troll-targeting-small-businesses.
[5] Love, Brian J. and Lefouili, Yassine and Helmers, Christian, *Do Standard-Essential Patent Owners Behave Opportunistically? Evidence from U.S. District Court Dockets* (November 8, 2020), 17, https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2020/wp_tse_1160.pdf/.
[6] *See In re Nimitz Technologies LLC*, No. 23-103 (Fed. Cir. 2022); *see also* https://www.unifiedpatents.com/insights/2023/2/21/litigation-investment-entities-the-investors-behind-the-curtain.
[7] https://news.bloomberglaw.com/business-and-practice/fortress-billions-quietly-power-americas-biggest-legal-fights.

III. *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 mandating the use of the WLAN Authentication and Privacy Infrastructure (WAPI) Chinese national standard to undermine Wi-Fi and restrict access to the Chinese market[8]). 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 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. Unfortunately, many of their efforts have been successful. Today's framework of SEP laws and policies, both in the United States and abroad, allow foreign adversaries and their proxies that hold key SEPs to abuse their market position by, for example, enabling the locking out of U.S. competitors from entering entire markets.

The SEP licensor abuse playbook is well-practiced. SEP abuses that have taken place in telecommunications markets for well over 20 years 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.

SEP abuses also represent one of the most glaring vulnerabilities to 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 wireless communication standards refuse requests for FRAND licenses from reasonable and willing licensees. Instead, the SEP abusers 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 license 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. This result has forced manufacturers in mature supply chains, such as in the automotive industry, to revert to using earlier versions of wireless communications standards (e.g., 3G or 4G for telematic control units) and limit the number of alternative suppliers to choose from to support a resilient supply chain. 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 leveraged to solidify controlling roles in critical U.S. supply chains. Disruptions to supply chains caused by SEP licensor abuse 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

[8] https://actonline.org/2016/03/17/mobile-mythbusting-wifi-wapi-and-the-encryption-debate/.

disrupting mature supply chains.

A. *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.[9] In 2019, the U.S. Department of 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, 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.[10] 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 claimed 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:

- 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), even though only 7 percent of the relevant patents were UK patents.[11]

- Since 2022, Huawei has sued the **Stellantis** automotive group (Fiat, Opel, Peugeot, and Citroën) in the German court system alleging SEP infringement, significantly disrupting automotive supply chains.[12] Auto manufacturer Continental has detailed the impacts of SEP abuses on the industry.[13]

- 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.[14] **NETGEAR** was

---

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

[10] https://www.iam-media.com/article/huawei-transfers-766-3gpp-related-patent-assets-new-npe.

[11] https://www.law360.co.uk/articles/2267824.

[12] https://www.lexology.com/library/detail.aspx?g=b6466f6d-b998-4e85-a96c-de3e06da7719.

[13] https://www.regulations.gov/comment/USTR-2023-0014-0040.

[14] https://ipfray.com/new-huawei-v-netgear-filings-discovered-in-munich-and-upc-interim-conference-to-take-place-next-week-wifi-6-seps/.

forced to sue Huawei in California federal court under a civil Racketeer Influenced and Corrupt Organizations Act (RICO) claim in response to Huawei's UPC suit weaponizing its SEPs to obstruct U.S.-based NETGEAR from complying with international standard

- Huawei's established strategy includes weaponizing jurisdictions abroad where injunctions on SEPs can be improperly attained,[15] including Brazil where Huawei has already made 1,794 patent applications since 2018.[16]

The above examples are only what is known from public reporting, and Huawei's activities, emboldened by a lack of U.S. leadership in SEP/FRAND licensing policy, 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 agreements that prohibit revealing their abusive terms. Further, 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.[17] 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

B*. 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:

- **Establish an Administration policy** that FRAND royalties are based on the intrinsic value of the patented technology, not the cost of market exclusion. This policy should reinforce key case law, such as the U.S. Supreme Court's *eBay v. MercExchange* ruling, which limits injunctions to protect U.S. innovation from bad-faith patent holders. Additionally, the policy should strengthen mechanisms like the Patent Trial and Appeal Board (PTAB) to enable the challenge of vague or invalid patents and prevent frivolous enforcement.

- **Increase antitrust enforcement** and leverage sanctions, tariffs, and other **restrictions** against entities that abuse SEPs, holding technical standards hostage and harming American businesses, consumers, and supply chains.

- **Implement measures to limit foreign abuse** in SEP licensing by holding foreign entities, like Huawei and its adversaries, accountable for unfair practices, ensuring that SEP holders adhere to FRAND commitments, and preventing the exploitation of U.S. markets through anti-competitive licensing strategies.

---

[15] https://www.iam-media.com/article/inside-huaweis-americas-ipr-department.
[16] https://www.iam-media.com/article/the-top-chinese-patent-holders-adding-brazil-their-strategic-maps.
[17] https://www.sisvel.com/news/huawei-joins-sisvel-cellular-iot-patent-pool/.