September 28, 2017

The Honorable Robert E. Lighthizer
United States Trade Representative
600 17th Street, N.W.
Washington, DC 20508.

RE: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation (Docket No. USTR-2017-0016)

BSA | The Software Alliance (BSA)[1] is grateful for the opportunity to provide comments to the United Stated Trade Representative (USTR) on the experience of its members in relation to technology transfer, intellectual property protection and enforcement, market access, and innovation policies and practices in China.

BSA is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, and are global leaders in advancing cybersecurity. Many of its members have significant and long-standing presences in China, and have seen first-hand the challenges and evolution of China's policies in the technology sector.

I. Introduction

As the United States' largest trading partner and the world's second largest economy, China presents US companies with important opportunities for reaching new consumers and pursuing new directions in innovation. In China, as in other nations, BSA seeks a policy environment that is (a) transparent, fair, consistently enforced, and (b) aligned with international laws, standards, and commitments. Our members also seek to promote strong bilateral relations between the United States and China that facilitate mutual exchange of commerce and investment that brings tremendous benefits to both the Chinese and American people. As USTR conducts its investigation, BSA proposes these twin objectives as guideposts for further action.

A fair, transparent, consistently enforced, and internationally-harmonized policy environment in China is critical to ensuring that there is a level playing field on which foreign companies operating in China can compete in a manner that does not undermine

[1] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Docusign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

their critical investments into the research and development of valuable intellectual property. China's compliance with its obligations as a member of the World Trade Organization (WTO) and with key bilateral and multilateral commitments represents an especially important indicator of its commitment to a rules-based trade framework.

In the decade and-a-half since China acceded to WTO membership, it has unquestionably made progress in revising its laws and economic policies to address concerns about market access and state intervention in the economy. China has undertaken an impressive series of legislative actions, including revising old laws and developing new laws, to establish a clearer, more coherent legal framework governing China's economy. In several instances, this framework has enabled China to make strides toward a rules-based trading system consistent with WTO and other international obligations. However, BSA and its members continue to have significant concerns about a range of Chinese policies and practices that substantially hamper market access and competitiveness for BSA members. Some of these practices create market entry barriers, undermine intellectual property, threaten innovation, and create barriers to fair competition with domestic businesses.

In this submission, BSA commends several specific areas of concern to USTR for further examination as it proceeds with its inquiry. These areas of concern, detailed in the next section, represent challenges that BSA has highlighted for many years, and that have forced many companies either to enter the Chinese markets on unfavorable terms, including with respect to the transfer to technology and intellectual property, or to withdraw from China altogether.

It is important that these concerns be addressed in a way that can achieve mutual progress toward strengthening the US-China relationship and trade between these two nations. Despite the challenges that have given rise to this inquiry, the US-China trade relationship is foundational to the present and future of the US economy, as our businesses are inextricably intertwined with the Chinese market. Not only do US businesses sell a range of products and services to Chinese consumers; China is also increasingly a critical center of the global supply chain, a hub of scientific and technological innovation and cooperation, and a critical global stakeholder in information technology governance. We are eager to see USTR pursue the below concerns in a dialogue with the Government of China that can lead to meaningful solutions to the problems identified and a sounder mutual foundation for addressing concerns going forward.

II. Specific Areas of Concern

China has benefitted as much as, or more than, any other country in the world from global digital commerce, with foreign suppliers helping China develop its own thriving technology industry and helping to connect and empower hundreds of millions Chinese citizens by making the world's most innovative technologies accessible to them. Yet, in many instances, the Chinese government has established policies and practices relating to intellectual property and market access that prevent foreign businesses from operating in China efficiently, or at all, and fail to protect the intellectual property and trade secrets of those companies that do operate in China.[2] These barriers stifle domestic innovation,

[2] The use of unlicensed software remains a problem in China. According to BSA's 2016 Global Software Survey (http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf), the rate of unlicensed software use in China declined from 74 percent in 2013 to 70 percent in 2015. This rate remains far above regional (61 percent) and global (39 percent) rates. The estimated commercial value of unlicensed software in China was nearly $8.7 billion USD in 2015. BSA notes recent actions by

undermine global commerce, threaten companies' most valuable assets, including their ability to compete fairly, and inhibit China from tapping into the full potential of global digital commerce.

China's market access barriers are particularly acute in relation to cloud computing and other leading-edge data services that depend upon the unfettered flow of data across borders. In a globalized economy, companies across all sectors rely on the Internet to transmit and receive data to operate and serve their customers. Recent regulatory rules in China are clamping down on data flows, making it difficult and unpredictable for companies that operate in the Chinese market. It is worth noting that market access barriers often work in tandem with pressures or requirements to transfer technology or intellectual property: in many cases, companies may only access the Chinese market through arrangements – from joint venture requirements to source code disclosure regulations – that put their intellectual property at unreasonable risk. US businesses thus often face a Catch-22: either they must risk their intellectual property or be closed out of the world's largest market for technology products.

We comment below on four areas of particular concern to BSA members because of the significance of their impact on the industry: (A) Foreign Direct Investment Restrictions, including policies relating to Value-Added Telecommunications Services; (B) Restrictions on Cross-Border Data Transfers; (C) Requirements for Source Code and Enterprise Standard Disclosure; and (D) Reliance on Indigenous Technical Standards.

A. Foreign Direct Investment Restrictions

US businesses seeking to operate in China are subject to a range of foreign direct investment restrictions, including equity caps, investment restrictions, in-country hosting requirements, and other similar regulations, as well as challenging processes for obtaining licenses and other prerequisites for entering the market. These restrictions are particularly acute for the telecommunications and information technology industries, including for cloud computing services, which are considered "value-added telecommunications services" under Chinese law.

China defines basic telecommunication services (BTS) and value-added telecommunication (VATS) as restricted industries for foreign investment. For BTS, the proportion of foreign investment may not exceed 49 percent. For VATS services, foreign firms in China can only operate through joint ventures, of which they may own no more than 50%. This restriction limits the ability of US businesses to freely make decisions on how to best advance their business operations in China, as well as their ability recoup substantial investments required to enter the market. The State Department's 2017 *Investment Climate Statement* for China notes, "the relative opacity of the approval process and the broad discretion granted to authorities foster an environment where the Chinese government can impose deal-specific conditions beyond written legal requirements, often with the intent to force

---

China to improve enforcement of intellectual property rights, such as the establishment of five specialized intellectual property courts and the implementation of court procedures supporting evidence preservation, but believes further measures are necessary to address unfair competitive disadvantages of U.S. businesses impacted by widespread software piracy.

technology transfer as a condition of market access or to support industrial policies and the interests of local competitors."

In December 2015, the Chinese Ministry of Industry and Information Technology (MIIT) issued China's *Telecom Services Catalog*, which entered into force on March 1, 2016. The revised *Catalog* continues to treat cloud computing and other Internet-based services as VATS. The designation carries significant restrictions on foreign investments. For example, companies wishing to provide web- or cloud-based content services must acquire an Internet Data Center (IDC) license. By regulation, foreign firms wishing to acquire such a license must establish a foreign invested telecommunication entity (FITE), which must contain no more than 50 percent foreign equity. BSA understands that MIIT issues very few new IDC licenses to FITEs.

Building on the *Telecom Services Catalogue*, in December 2016, MIIT released a draft *Notice on Regulating Business Behaviors in the Cloud Service Market*. While this regulation remains in draft form, it would further constrain the ability of foreign businesses to partner with domestic entities, introducing an unprecedented level of government interference into these partnerships without articulating any clear rationale. This draft *Notice* would place a number of restrictions on technical partnerships between foreign cloud services operators and domestic IDC license-holders. For example, it would mandate that the operator cannot lease or transfer its VATS license, or provide resources, premises or facilities to its partner. It would also, as discussed below, require localization of data as well as of cloud service platforms and service centers. These restrictions could undercut many, if not most, agreements that foreign technology companies currently have in place for providing cloud services in partnership with IDC service providers.

Regulations governing VATS are exacerbated by additional Chinese policies. China's *Multi-Level Protection Scheme* (*MLPS*) imposes significant restrictions on procurement of software and other information security products for an overly broad range of information systems the government considers sensitive. Among other requirements, procurements of such products are limited to those with intellectual property rights owned in China. This applies to procurements by the Government of China and increasingly to procurements by state-owned enterprises (SOEs) and private sector entities, restricting market access for foreign information security products. As a result, foreign companies are denied market access and many entities in China are unable to procure the most effective security tools to meet their needs.

In addition, technology businesses are subject to insufficient and contradictory laws relating to contracts and liability for infringement. Article 24 of China's *Technology Import and Export Regulations* mandates that technology importers indemnify their customers and bear the liability for infringement. In contrast, Article 353 of China's *Contract Law* permits the parties to negotiate who will bear liability for infringement, but Article 355 states that, for a technology import and export contract, the *Regulations* shall apply. This lack of freedom of contract discriminates against overseas licensors and could be viewed as a non-tariff technical barrier.

Finally, while these policies themselves create specific concerns, particularly in relation to licensing requirements that bar foreign businesses from competing in China on equal terms with domestic entities, the implementation of these policies can be equally concerning, and far more difficult to document. US firms attempting to provide cloud computing or other VATS services must navigate a licensing process that can be lengthy, unpredictable, burdensome, and discriminatory. Businesses have encountered requirements or pressure to disclose intellectual property, inconsistent interpretation of regulations between central

and local regulators, lengthy or open-ended approval timelines, and a lack of transparency around decision-making while navigating the licensing process. These concerns represent a significant barrier to foreign access to the Chinese market.

B. Restrictions on Cross-Border Data Transfers

The Chinese government has put in place a number of laws and regulations restricting the free flow of data across borders and forcing data to be stored locally. For US businesses that provide cloud computing services, or rely heavily upon cloud computing for their business operations, these restrictions create an uneven playing field, advantaging domestic businesses that already have local infrastructure, and preventing foreign businesses from operating efficiently, or at all. We summarize key laws and regulations impeding cross-border data flows below.

Critical Information Infrastructure Restrictions

Article 37 of China's *Cybersecurity Law* requires that "personal information and other important data gathered or produced by critical information infrastructure operators during operations" within China must be stored within China. Subsequently, the Cybersecurity Administration of China (CAC) issued *Draft Critical Information Infrastructure Protection Regulations* that contain an exceptionally broad definition of "critical information infrastructure" that would include cloud computing services. These *Regulations*, if enacted as drafted, would effectively require that all cloud computing services operating in China store data from their operations in China, thus creating additional operational costs and access challenges for foreign providers.

Cloud Service Regulations

On November 24, 2016, MIIT published a draft *Notice on Regulating the Operation Behaviors in the Cloud Service Market*. While this *Notice* has not yet been finalized, the draft contains several provisions that would serve as highly problematic market barriers to foreign cloud providers. Article 7 would require cloud suppliers to physically construct cloud service platforms in China, potentially forcing providers to create redundant infrastructure that drives up the costs of operations for foreign providers, with network separation requirements that create interoperability issues with their global cloud infrastructure. Likewise, Article 9.4 would require cloud providers to ensure that network data and service facilities are located in China, and would subject cross-border data transfers to a range of restrictions. Article 10.3 of the *Notice* would require cloud service operators to create duplicate copies of all key equipment, business systems, and data, potentially making it cost-prohibitive and operationally impractical for foreign cloud providers to operate in China. Ultimately, this regulation would systematically increase restrictions on the ability of foreign cloud service providers to participate on equal terms within the China market, as well as their ability to partner on reasonable terms with Chinese companies.

Security Assessment Measures for Cross-Border Transfers of Personal Information and Important Data

On April 11, 2017, CAC issued draft *Security Assessment Measures for Cross-Border Transfers of Personal Information and Important Data* for public comment. While the measures remain in draft form, if implemented, they would impose additional restrictions on the transfer of data across borders, including limiting the remote access of data stored in China from outside of China. Article 2 of the draft would require all "personal Information" and "important data" generated or collected by network operators in China to be stored

domestically. Personal information is defined more broadly than accepted international standards, and the definition of "important data" is so broad and vague as to leave significant uncertainty about what data is covered and how this requirement aligns with regulations relating to "critical infrastructure information" as governed by the *Cybersecurity Law*. While the draft measures do include the possibility to transfer such information extraterritorially upon completion of a security assessment, the uncertainty about definitions of covered data and obligations relating to security assessments creates unacceptable legal risk for cloud providers depending upon cross-border data flows for their business operations, and – if adopted in current form – will serve as another key barrier to digital commerce.

C. Requirements for Source Code and Enterprise Standards Disclosure

Through a series of draft and final legislative documents on various topics spanning the last several years, the government of China has made clear its intention to establish a legal basis for requiring the disclosure of source code and enterprise standards associated with foreign software products across a wide range of uses. Requirements for the disclosure of source code and enterprise standards pose significant inherent risks to intellectual property; moreover, such disclosures provide little security value. While the government has begun taking action to implement source code disclosure requirements, many such requirements have either not been finalized or have not been developed with sufficient clarity on their extent and procedures; it is critical that the government intervene to eliminate current disclosure requirements and arrest further advancement of draft requirements.

The most significant measure relating to source code disclosure is China's *Cybersecurity Law*, which includes requirements that products associated with "critical infrastructure information" be subject to security reviews. On May 2, CAC published a final version of new *Trial Measures for Security Review of Network Products and Services*, intended to implement the *Cybersecurity Law* security review requirements. The measures mandate that all "important network products and services" purchased for national security-related systems will be subject to security reviews, though the measures do not define "important network products and services" or delineate what systems are national-security related. The measures direct that the security reviews will focus on whether products are "secure and controllable," but leave determinations about whether source code disclosures will be required to future implementing regulations. The possibility that source code disclosures could be mandated through these security reviews is cause for substantial concern among BSA members and other US companies.

Likewise, Chinese regulators are considering source code disclosure requirements in the area of cryptography. On April 13, 2017, China's State Cryptography Administration (SCA) published a draft *Encryption Law* for public comment. The draft law is concerning for several reasons. First, it would fully or partially bar foreign competition in various categories of cryptography: of the three categories defined by the law (core, common, and commercial cryptography), foreign businesses would only be allowed to participate in the commercial cryptography market, and there only under strict regulations.

Second, the draft law lacks a clear definition of the scope of commercial cryptography, leaving significant uncertainty about which products and services foreign companies might provide. Third, the licensing scheme for foreign commercial cryptography providers, as envisioned by the draft law, would require such providers to disclose source code to state licensers, putting their intellectual property at significant risk. Finally, the law requires the Chinese government to develop and apply mandatory national technical standards which,

as noted below, run counter to China's commitments under the WTO Agreement on Technical Barriers to Trade (TBT Agreement).

Equally concerning is the possibility that China may require mandatory disclosure of enterprise standards. On March 22, 2017, China' State Council Legislative Affairs Office (SCLAO) published a draft *Standardization Law* that would represent the first amendment to China's *Standardization Law* since its original passage in 1989. This draft addresses enterprise standards, which it describes as an individual company's proprietary product or services specifications. These specifications represent highly proprietary, confidential information that often is protected by trade secret law or other forms of intellectual property.[3] The draft law would require the public disclosure of enterprise standards, a practice that would prove exceptionally damaging to the integrity of intellectual property held by US technology companies.

No other country in the world requires public disclosure of comprehensive lists of technical standards used in products or services. Not only would such disclosure compromise valuable intellectual property; it would also establish a significant cost burden on businesses. Because application of certain specifications and standards varies from product to product, the engineering and legal verification overhead for such a disclosure requirement would be significant, likely driving some companies out of the market altogether.

D. China-Specific Technical Standards

Internationally recognized and adopted technical standards that are established with industry participation and accepted across markets generate efficiencies and speed the development and distribution of new products and services, allowing consumers to get them faster and at lower cost. Government intrusion into and manipulation of standards-setting processes hampers innovation and creates artificial barriers to trade. The WTO TBT Agreement, as well as the TBT Agreement Code of Good Practice, to which China is party, make clear that member nations are expected to utilize international standards, wherever they exist, as the basis for technical regulations. For example, Article 2.2 of the TBT Agreement states that, "Where technical regulations are required and relevant international standards exist or their completion is imminent, Members shall use them, or the relevant parts of them, as a basis for their technical regulations except when such international standards or relevant parts would be an ineffective or inappropriate means for the fulfilment of the legitimate objectives pursued...."[4]

The TBT requirement to use international standards is critical to international free trade because indigenous technical standards can serve as barriers to foreign companies seeking to access a market by forcing foreign companies to accept significant increases to

[3] China does not currently have a standalone trade secrets law, and trade secrets remain one of the most at-risk types of intellectual property for US businesses operating in China. While companies do have legal recourse to pursue cases of trade secrets violations, existing procedures make it difficult for victimized businesses to achieve any favorable legal resolution. This most significant challenge is difficulty companies face under the Chinese court system in establishing a valid and effective evidence chain, due to the complexity of evidence rules and rules governing the burden of proof. It is critical that China develop a standalone trade secrets law to afford adequate protections to foreign businesses, provide clear and fair rules regarding evidentiary chains and burden of proof, and ensure sufficient enforcement.

[4] World Trade Organization, "Agreement on Technical Barriers to Trade," 1868 U.N.T.S. 120. https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm.

production costs associated with redesigning products to meet varying indigenous technical standards. Moreover, indigenous technical standards are often used to protect domestic firms and insulate them from foreign competition.

While international standards not only exist, but are widely used, in the technology sector, China is aggressively seeking to establish and mandate indigenous technical standards to support development of its technology industry. It has sought to establish indigenous standards that (i) aim to displace global standards when mandated, (ii) create significant interoperability issues because they deviate substantially from global standards, and (iii) lack sufficient safeguards to protect the intellectual property at issue in standards-setting activities. China requires compliance with indigenous standards in some cases; in addition, there have been several instances in which China has set forth indigenous technical standards as voluntary, only to make compliance with these standards mandatory through subsequent administrative measures. China has adopted or sought to develop unique Chinese standards in areas including Internet protocols, 3G telecommunications services, wireless local area networks, digital audio and video, radio frequency identification technology, and encryption, among others.

Moreover, these technical standards are often developed without adequate transparency and participation rights for foreign companies. Foreign companies should have the same access to and voting rights in Chinese standards setting bodies as Chinese companies, and ensure that there is no "presumption of participation" in Chinese standards setting laws, rules or administrative regulations that would allow the Chinese government to unfairly procure the intellectual property of foreign companies on non-market or royalty free terms. They should be permitted to participate in Chinese standards-development efforts on an equal and non-discriminatory basis.

III. Conclusion: Achieving a Constructive Resolution

The concerns outlined in the previous section significantly impact the ability of BSA members and other US companies to do business in China on a level playing field. They impede the free flow of data that underpins the global digital economy, undermine innovation, and put valuable intellectual property at risk. As a direct result of these policies and practices, some companies have been driven out of the Chinese market altogether, while others have reached accommodations that enable continued participation in China's market but bring risk, uncertainty, and inefficiency.
Establishing a more equitable foundation for the US-China trade relationship is important; equally important is that these concerns be addressed in a way that can achieve mutual progress toward strengthening the overall health of this relationship. We are eager to see a constructive dialogue with the Government of China aimed at win-win solutions.

Specifically, BSA would prioritize the following issues to be addressed through such a dialogue:

(1) *VATS Licensing Requirements.* China has recently undertaken steps to liberalize restrictions on value-added services, but telecommunications and information technology products remain overly and unfairly restricted. Loosening restrictions to enable foreign businesses to compete in these arenas on a level playing field would represent a major advance with regard to reciprocal and fair market access.

(2) *Cross-Border Data Transfer Restrictions.* Loosening restrictions on cross-border data transfers is essential to ensure fair market access for businesses that depend on cloud computing and other data-centric technologies. Seeking to align China's definitions of

critical infrastructure information and personal information, which underpin many of its most problematic regulations, with international standards and best practices would go a long way toward achieving this priority.

(3) *Clarification of Security Reviews*. As previously noted, China continues to erect its architecture for conducting security reviews mandated by the *Cybersecurity Law* and other laws and policies, creating uncertainty about to what extent source code and enterprise standards disclosure will be mandated. Were China to clarify that source code and enterprise standards disclosure will not be required under security reviews, and that security reviews can be conducted by internationally accredited international third-party certification authorities, the confidence of technology businesses in China's review regime would increase substantially.

Addressing these concerns is of the utmost importance. BSA members are eager to see the Administration's investigation proceed in a way that is constructive and is aimed toward the goal of ultimately improving the US-China trade relationship. The US-China trade relationship is foundational to the present and future of US businesses, and it is critical that these concerns be resolved in a way that strengthens this foundation rather than incentivizing additional protective or retributive measures. For that reason, we are eager to see USTR pursue the above concerns in a dialogue with the Government of China that can lead to meaningful solutions to the problems identified and a sounder mutual foundation for addressing concerns going forward.

Sincerely,

Tommy Ross
Senior Director, Policy

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org