October 22, 2013

Filed via www.regulations.gov
Douglas M. Bell
Chair, Trade Policy Staff Committee
Office of the U.S. Trade Representative
Washington, DC 20508

Re: Request for Public Comments Regarding the National Trade Estimate Report on Foreign Trade Barriers, 78 Fed. Reg. 50481 (August 19, 2013) Docket: USTR-2013-0027

To the Trade Policy Staff Committee:

BSA | The Software Alliance (BSA)[1] appreciates this opportunity to provide comments to assist your preparation of the 2014 National Trade Estimate Report on Foreign Trade Barriers (the "NTE Report").

Introduction

Market access barriers in key foreign markets pose a significant and growing challenge for BSA members. Many of the fastest-growing IT markets in the world are where we are seeing the most troubling policies creating barriers to foreign software and other IT products and services. Access to these markets on reasonable terms is critical to the future growth of BSA member companies and to their ability to contribute to economic and job growth in the United States.

The trade barriers BSA members confront in foreign markets take many forms. These include poor protection and enforcement of intellectual property rights and many "behind-the-border" regulations that are often justified as policies to promote innovation, enhance security, or advance other domestic priorities, but in practice act as unjustified barriers to member company products and services.

[1] *BSA | The Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward. BSA's members include: Adobe, Apple, Autodesk, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Dell, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Oracle, PTC, Rockwell Automation, Rosetta Stone, Siemens PLM, Symantec, Tekla, and The MathWorks.*

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

To highlight one important example, as cloud computing becomes a central business model for many software companies, there has been a flurry of activity by governments in many global markets to create new rules and regulations that impact cloud products and services. In some cases, these rules and regulations pose barriers that impede the ability of IT companies to provide cloud products and services on a global scale. This includes efforts in a number of countries to impose restrictions on the free flow of data across borders, require the use of local servers, or adhere to unique national cloud and security standards, all of which raise the costs of such services and undermine the efficiency of this business model.

I. BSA Members Face Several Types of IT Market Access Barriers to their Products and Services in Global Markets

BSA members face an array of barriers to their products and services in key global markets. These include:

1. **Weak protection and enforcement of intellectual property rights,** including copyright, patents and trade secrets.

2. **Restrictions on cross-border data flows,** for example requiring suppliers offering cloud and other digital products and services to locate data centers in-country or restricting the ability of foreign-invested enterprises (FIEs) to run data centers.

3. **Discrimination in procurement by government agencies and state-owned or state-influenced enterprises** including mandates or preferences for domestically owned or produced products, for products utilizing a particular technology or business model, or for products whose intellectual property is owned or developed locally.

4. **Development of country-specific technology standards** to bolster domestic firms and insulate them from foreign competition.

5. **Overreaching security-related regulations** that limit market access for foreign information security and other IT products by mandating the use of local products or imposing unreasonable testing or certification requirements.

6. **Tariff barriers** that persist because many countries have not joined the Information Technology Agreement (ITA), and the agreement does not cover important new categories of software and hardware.

In 2012, BSA released a report detailing many of these trade barriers, along with case studies of particular policies of concern.[2]

[2] *Lockout: How a New Wave of Trade Protectionism Is Spreading through the World's Fastest-Growing IT Markets – and What to Do about it* (June 2012), available at www.bsa.org/tradelockout.

II. Specific Examples of IT Market Access Barriers in Key Markets

Below we highlight several examples of particularly troubling market access barriers to our members' products and services in key markets. We focus here on China, India and Brazil, three of the fastest-growing markets for IT products and services, though these are by no means the only markets where BSA members face these barriers. Even within these markets, these examples are not an exhaustive list of problematic policies, but illustrative of how IT market access barriers are being put into practice in priority markets. We also highlight specific examples of the emerging barriers to cloud computing we are seeing in many markets.

We focus in this submission primarily on non-IP related barriers. The significant IP-related market access barriers BSA members confront in key markets are detailed in separate submissions made by the International Intellectual Property Alliance (IIPA), which BSA is a member of, for the Special 301 process and the NTE Report.[3]

China

Government procurement of software

In May, China's Ministry of Finance (MOF) issued a new directive on government procurement of software that could significantly restrict market access for foreign software products and services. The directive would impose price controls, preferred licensing terms (such as a preference for a "business premise" (site) license), minimum terms for software life and other requirements on procurement of software that would have the effect of discriminating against the purchase of foreign brands. Moreover, the directive defines "standard configurations" of desktop software to include only operating system, office productivity and anti-virus software suggesting that procurement may not be authorized or, at a minimum, that budget will not be made available for other types of software.

This directive does not comport with best practices for software procurement and does not adequately take into account the speed with which software products and services are developing. Moreover, it puts in place de facto preferences for procuring domestic software products and services that are not in keeping with China's commitments in bilateral negotiations with the United States and its WTO accession obligations. In the US-China Joint Commission on Commerce and Trade (JCCT) and US-China Strategic & Economic Dialogue (S&ED), the Chinese government has made numerous commitments to avoid discrimination against foreign products with foreign-owned or foreign-developed intellectual property in its government procurement. China's WTO accession obligations include commitments to prohibit imposition of new price controls that apply to government and non-government procurement (notably, the MOF procurement rules appear to cover some SOE procurement as well as government procurement). The recently issued MOF software procurement rules pose a significant barrier to US software sales in China and are contrary to China's bilateral and WTO commitments.

[3] IIPA's Special 301 and NTE submissions are available at www.iipa.com.

Multi-Level Protection Scheme (MLPS)

China's MLPS mandates that only Chinese-owned information security and other IT products with core IP that is Chinese-owned can be used in a broad array of information systems the Chinese government considers sensitive (*i.e.*, those classified as Level Three or higher). The policy takes a broad view of sensitive systems classified at Level Three or higher that could sweep in a wide array of enterprises and government agencies in the areas of finance, transportation, telecommunications, health, education, and other industries. We welcome China's commitment in the 2012 JCCT that it "will conduct a process to revise this measure and seek the views of all parties, including through dialogue with the United States." To date, we are not aware of any efforts by the Chinese government to move forward with this process. We would like to see China conduct an open and consultative process to review and revise the MLPS. This would include convening technical dialogues with US government and industry to discuss best practices for protecting sensitive networks, with a focus on China removing requirements for Chinese-owned IP for Level Three and above commercially oriented systems along with any requirements for mandatory product testing in government-affiliated laboratories.

Moreover, according to the Guideline of the Commercial Encryption Products Management, all encryption products should undergo prior examination and approval, and FIEs have to work with domestic vendors with licensees for encryption modules. The practice is not in line with international norms and limits the flexibility to serve customers.

Telecom Services Catalogue

Earlier this year, China's Ministry of Industry and Information Technology (MIIT) issued proposed revisions to the Telecom Services Catalogue. The revisions attempt to classify cloud computing and other Internet-based IT services as value-added telecom services (VATS). If this classification system is imposed, many services offered by software companies, e.g., cloud computing, content delivery, information security services and call centers, will be subject to telecom regulatory requirements including foreign investment restrictions and more burdensome licensing rules. These types of IT services should not be treated as VATS and should be left outside the telecom regulatory system. Even where such services are Internet-based and/or use telecom networks (such as optical fiber networks), the nature of such services are not fundamentally telecom services. Imposing telecom regulations on these services will limit market access for foreign companies and inhibit the growth of these services in China.

ICP and IDC Licenses

In order to provide commercial Internet content services in China, companies must have an internet content provider (ICP) license, a type of VATS license. Foreign companies wishing to get a VATS license must enter into a foreign invested telecommunications enterprise (FITE) where foreign investment cannot exceed 50 percent. We understand MIIT has essentially ceased issuing ICP licenses to FITEs, forcing many US companies to enter into contractual relationships with Chinese entities that already hold an ICP license. These licensing restrictions significantly undermine the ability of foreign companies to offer cloud computing and other

Internet-based products and services in China. Similarly, running data centers is strictly regulated and in practice FIEs have no opportunity to get the license (an IDC license), which significantly limits the ability to offer cloud services in China.

Other Cloud Computing Impediments:

- China's TC260 has published new Cloud Security Standards that contain many problematic provisions including requirements to disclose sensitive and valuable intellectual property and unworkable supply chain language, among others. The process of drafting these standards is closed to foreign participation.
- Extensive regulation of internet content, including mandatory filtering and censoring. This includes China's "Great Firewall" which frequently operates to block or slow access to services hosted outside of China without clear criteria as to when a site will be blocked or clear procedures to contest the blocking or delayed access to a site.

Patent Law Reform

The Chinese government is currently undertaking a process to amend the Patent Law, led by the State Intellectual Property Office (SIPO). Among other things, the proposed amendments would give expanded enforcement powers to SIPO, who may be able to conduct "ex officio" raids and enforcement actions against ill-defined "market-disruptive" patent infringement activities, and award fines as well as compensatory and punitive damages. This creates enormous risks for foreign patent holders in China. The Chinese judicial system is the proper forum to adjudicate patent infringement and damages, and it does not make sense to vest that same authority in administrative agencies as well.

The proposed empowerment of SIPO and hundreds of local intellectual property offices (IPOs) in enforcing patents will dramatically change the current enforcement landscape, creating the potential for substantial confusion and duplication of the role that courts now play. The envisioned role for SIPO and IPOs as patent enforcement authorities is, based on our research, without analogue in any other national law.

While we understand the focus of this round of amendments is on patent enforcement, we would hope the Chinese government could address priority patent issues that are of key concern to domestic and international industries, such as the patentability of graphic user interfaces and changing substantive patentability criteria for utility model patents. These changes would help stimulate the growth of the technology sector in China.

Five-Year Plans and Strategic Emerging Industries (SEIs)

More generally, China's current Five-Year Plans and Strategic Emerging Industries initiatives for IT sectors lay out a clear intent to use various policy levers to bolster domestic industries and raise serious concerns that they will be implemented in a manner that discriminates against foreign companies. For the most part, these plans have not been made available for public comment and most have not been published, even if they are finalized.

India

Procurement Preferences

In February 2012, the Ministry of Communications and Information Technology issued the Preferential Market Access (PMA) Policy which imposes local content requirements for the procurements of IT and telecommunications hardware products. Under the rules, US ICT companies would be forced to source a percentage of all hardware products in India, or risk being disqualified from procurement contracts.

As originally proposed, the PMA would impose these procurement restrictions on both government and certain private sector government licensees. If implemented in this manner, this policy would represent an unprecedented interference in the operations of private companies, create enormous disruptions in key sectors of the Indian economy and significantly undermine the ability of American companies to compete fairly in India.

After significant concerns were raised by the US and other foreign governments, the Prime Minister's Office announced in July that it was suspending implementation of the PMA and reassessing it. At that time, the PMO indicated that the domestic content requirements would not be applied to government licensee procurement. We understand that a new policy has been approved by the Cabinet, but the details are not yet known.

Safety and Security Testing Requirements

Over the past year, the Ministry of Communications and Information Technology issued new requirements for safety and security testing and certification for all imported electronic products. The new safety and security testing requirements deviate significantly from international best practices and norms and have already created enormous disruptions for global ICT companies.

Among the problematic requirements is that products must be tested in designated labs in India, regardless of whether the products have already been tested and certified by internationally accredited labs. This imposes a major and unwarranted requirement on foreign IT companies in particular, and inadequate lab capacity in India has led to extensive backups at Customs

The new safety testing requirements had been set to take effect for certain ICT products in October. Due to significant international concerns raised about the requirements, they have been postponed by three months (to January 2014). The security testing requirements were set to go into effect October 1, 2013, but no implementing guidelines or details have been provided.

Patent Reform

India recently issued draft Guidelines for Examination of Computer Related Inventions. The strict regime of patentability implemented by the Guidelines would disallow patent protection for innovations, including those having inventive technical character, in a vast segment of the

computer-technology field. Thus, the Guidelines do not appear to be consistent with Article 27.1 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, which states that patents shall be available for inventions in all fields of technology, assuming they satisfy the other criteria for patentability such as novelty, inventive step and industrial application. The regime implemented under the Guidelines would have a deleterious effect on the emerging software sector in India as well as on investment in India by multinational software companies.

Brazil

Procurement preferences

In August 2012, Brazil's Ministry of Science, Technology and Innovation released its "Bigger IT Plan" to encourage growth in the domestic IT industry. The plan focuses heavily on software and related services and includes a new process (the "CERTICS" program) to evaluate and certify software products that are locally developed in order to qualify for government procurement price preferences that could be as high as 25 percent.

BSA's concerns with the CERTICS program and implementation plan include vague criteria, eligibility on a per-product basis, short update horizons, and certification available only to software developed in Brazil by Brazil-based companies holding all IP to the software in Brazil.

CERTICS was scheduled to enter into force 60 days after publication on June 19, 2013, but has been delayed, in part to train inspectors. BSA urges delay of implementation of the program and consultations with industry on alternative means to encourage local software and IT development.

Data localization

Members of the Brazilian Administration and Congress are pushing to include restrictions on cross-border data flows and server localization requirements in pending internet regulation legislation (the "Marco Civil" bill) for the stated goal of protecting the privacy of Brazilian citizens. In August, the Brazilian House Science and Technology, Communication and Computing Committee held several public hearings to discuss the Marco Civil bill. Some in the Brazilian Congress and Administration used these opportunities to demand stronger privacy protections, including restricting cross-border data flows. As the bill remains under consideration in the House, we are closely monitoring developments and urging that no overly restrictive data localization requirements be included.

III. Emerging Barriers to Cloud Computing

Cloud computing offers many potential economic benefits. Via the cloud, small- and mid-sized organizations can access powerful computing resources once available only to the largest companies without having to make significant upfront investments in IT installation, maintenance, and support. Because many cloud service models charge on a "pay-as-you go"

basis, the cloud also enables organizations to scale usage up and down as needed. In these and other ways, the cloud can help reduce IT costs and be a powerful productivity enhancer for enterprises in all countries.

Rules restricting cross-border data flows undermine the cloud computing model. While clouds can be located on premises or contained within a given jurisdiction, cloud computing often involves the storage and processing of data in multiple locations and even in multiple countries. Indeed, many of cloud computing's primary advantages — such as reliability, resiliency, economies of scale, and 24-hour service support — can require that data be stored in multiple markets. Confining data within a given country inhibits the ability of cloud service providers to offer these benefits.

Policies that unnecessarily restrict the free flow of data or require use of local servers to offer cloud services prevent domestic and foreign cloud service providers alike from hosting data in third countries. But such policies often have a disproportionate impact on foreign cloud providers, whose primary data centers are more likely to be located outside of a given country. At a minimum, foreign providers may mirror data on servers in other jurisdictions as backup in case a domestic data center or national network fails.

Today we are seeing many countries adopting or considering policies that would restrict cross-border data flows, require the uses of local servers, or otherwise limit the ability to offer cloud and other digital products and services.

Restrictions on cross-border data flows

- **Argentina**, **Australia**, **Brazil**, **Canada**, **Chile**, **China**, **Colombia**, **Costa Rica**, **Greece**, **Hong Kong**, **India**, **Indonesia**, **Korea**, **Mexico**, **Peru**, **Russia**, **Switzerland**, **Vietnam:** All have adopted or proposed rules that prohibit or significantly restrict companies from transferring personal information out of the domestic territory.
- **Indonesia:** The government in 2012 introduced new electronic commerce regulations including provisions requiring providers to register their services with a central authority and rules that will force some providers to establish local data centers and hire local staff. Rules implementing these regulations are anticipated in 2013.
- **Vietnam:** The government recently adopted Decree No. 72 on Internet services requiring that at least one server be located in Vietnam in order to (i) establish an online social network, (ii) establish a general information website, (iii) supply content services on mobile telecommunications network, or (iv) provide online gaming services. In addition, there are also licensing and registration requirements in the Decree that could significantly restrict the ability to conduct cross-border data business. A separate IT Services Decree is under consideration by the government and could include similar problematic provisions.
- **India:** In May, the Government released its Cloud Strategic Direction Paper and Adoption and Implementation Roadmap. The purpose of these papers was to provide a strategic direction and implementation plan for putting in place cloud-based services for the government. A government committee including representation by some Indian industry associations is now working to recommend an overall policy framework for

private sector participation in the cloud. How both of these efforts will address data transfer and data localization is under active consideration and will impact the ability of US and other foreign companies to access the Indian cloud market.

- **European Union:** The EU is undertaking a review of the Data Protection Regulation and data protection Safe Harbor which currently allows thousands of companies in the US and EU to conduct business involving data transfers across the Atlantic. Some of the changes to these policies under discussion could significantly disrupt the ability of US companies to provide cloud and other services in the EU market that rely on cross-border data transfers. We encourage a fair and balanced approach to reform in this area that enhances privacy and maintains vibrant transatlantic trade in the many sectors of the economy that depend on data transfers.

Cloud-focused standards

BSA is closely monitoring the emergence of security, privacy, and cloud computing focused standards in the context of various standards organizations, within Codes of Conduct, and as part of procurement guidance. As cloud technology develops, ensuring use of commonly agreed global standards in this area is critical. For example, as noted above, **China's** TC260 has published new Cloud Security Standards that contain many problematic provisions including requirements to disclose sensitive and valuable intellectual property and unworkable supply chain language, among others.

We are also concerned that Codes of conduct, written and informal cloud computing guidance from data protection authorities (DPAs), and procurement model contract provisions just for cloud providers, undermine confidence in the technology and perpetuate a false belief that foreign Internet-based technologies, and cloud in particular, is unsafe for domestic consumption. For example, **New Zealand's** Cloud Computing Code of Conduct includes a provision requiring disclosure of data location. Companies provide this information to customers in the normal course of business transactions. By adding this to the New Zealand Code of Conduct, the Code serves to highlight it as a risky activity that customers should assess. The **EU's** Cloud Industry Select Groups are examining cloud computing in three different ways – through a Code of Conduct Group, through a standards and certification group and through a group looking at service level agreements (SLA). In each case, the recommendations and focus of the groups have moved towards data flow issues. Indeed the work has been referred to the Article 29 Committee for review. While not proposed specifically within these working groups, there is also a movement to create a data processing area within Europe closed to foreign business participation.

In February, BSA issued its second Global Cloud Computing Scorecard, a comprehensive assessment of the cloud "readiness" of 24 global markets.[4] The Scorecard analyzes and ranks these markets on the basis of their laws and regulations in seven areas: data privacy, cyber-security, cyber-crime, intellectual property, technology interoperability and legal harmonization, free trade, and IT infrastructure. The Scorecard and other BSA analyses will continue to track market barriers to cloud services in key markets.

[4] 2013 BSA Global Cloud Computing Scorecard (Mar. 2013), available at www.bsa.org/cloudscorecard.