



**Filed via [www.regulations.gov](http://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 to Compile the National Trade Estimate Report on Foreign Trade Barriers, 77 Fed. Reg. 49055 (August 15, 2012)  
Docket: USTR-2012-0021

To the Trade Policy Staff Committee:

The BSA | The Software Alliance (BSA)<sup>1</sup> appreciates this opportunity to provide comments to assist your preparation of the 2013 National Trade Estimate Report on Foreign Trade Barriers (the “NTE Report”).

In summary, BSA would like to highlight the following:

- Market access barriers to IT products are on the rise in the fastest-growing markets for IT products and services
- Generally these barriers involve non-tariff, “behind-the border” measures that are often justified as policies to promote innovation, enhance security, or advance other domestic priorities, but in practice act to discriminate against and disadvantage foreign suppliers
- The barriers affect both traditional software products, and new technologies like cloud products and services

**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 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 here in the United States.

---

<sup>1</sup> BSA | The Software Alliance ([www.bsa.org](http://www.bsa.org)) is the leading global advocate for the software industry. It is an association of more than 70 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, AVEVA, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Intel, Intuit, McAfee, Microsoft, Minitab, Progress Software, PTC, Quest Software, Rosetta Stone, Siemens PLM, Sybase, Symantec, and The MathWorks.

New personal computer (PC) sales in China now outstrip sales in the United States, and Brazil recently became the third-largest market for PCs, overtaking Japan. In fact, the four “BRIC” countries (Brazil, Russia, India, and China) now account for a quarter of all new PC sales globally, up from less than one-sixth in 2006. Given the rapid growth of these and other foreign markets for US IT products, the development of barriers to foreign IT products and services in these markets has an increasingly significant impact on the growth prospects for US and other global IT companies.

BSA and its member companies are seeing a growing wave of trade barriers to their products in key markets. While some of these involve tariff barriers, most take the form of in-country, “behind-the-border” regulations. They are often justified as policies to promote innovation, enhance security, or advance other domestic priorities, but in practice act as unjustified barriers to foreign suppliers.

To highlight one important example, as cloud computing becomes a central business model for many software companies, there has been a flurry of activity in global markets to create new rules and regulations to govern 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, which force cloud providers to offer country-specific cloud products and thereby raise the costs of such services and undermine the efficiency of this business model.

This past year, BSA released a detailed report identifying priority IT trade barriers our member companies face in emerging markets, along with case studies of particular policies of concern. The report also lays out recommendations for addressing these barriers. We highlight below key findings from the report and urge you to review the entire document at [www.bsa.org/tradelockout](http://www.bsa.org/tradelockout).

### ***1. 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. Among these are weak protection and enforcement of intellectual property (IP) rights. For a detailed inventory of the IP concerns our members face in priority markets, we refer you to the submission made by the International Intellectual Property Alliance (IIPA), which BSA is a member of, for the 2012 Special 301 process and IIPA’s submission for the 2013 NTE Report.<sup>2</sup>

In addition to IP-related barriers, BSA members must contend with several other types of market access restrictions that particularly impact IT goods and services. These include:

---

<sup>2</sup> Both the IIPA 2012 Special 301 Report and IIPA’s submission for the 2013 NTE Report are available at [www.iipa.com](http://www.iipa.com).

1. **Restrictions on 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.
2. **Manipulation of technology standards** to bolster domestic firms and insulate them from foreign competition.
3. **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.
4. **Regulatory obstacles to cloud computing** that unduly burden or discriminate against foreign firms by, for example, requiring suppliers offering cloud services to locate data centers in-country or by significantly restricting cross-border data flows.
5. **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.

## ***II. IT Market Access Barriers are Proliferating in Key Markets***

Below is an overview of how each of the market access barriers enumerated above is playing out in key markets. This paints a picture of a worsening market access landscape for BSA member products and services in some of the world's fastest-growing IT markets.

The case studies below are not an exhaustive list of the problematic policies our members face, but illustrative examples of how these market access barriers are being put into practice in priority markets.

### **1. Restrictions on Procurement by Government Agencies and State-Owned or State-Influenced Enterprises**

Given the size and importance of procurement by government agencies and state-owned or state-influenced entities, securing fair and open access to these markets is a high priority for IT suppliers. Measures that exclude multinational suppliers from access to government procurement and procurement by state-controlled or state-influenced enterprises translate into high levels of lost exports and jobs. They also deprive governments and other purchasers in these markets the ability to choose the best available IT products and services at the best prices. In many countries, governments are the single largest purchasers of IT products. Combined public sector spending on information and communications technologies worldwide in 2010 was estimated at \$423 billion.<sup>3</sup> In emerging economies in particular, governments tend to be disproportionately large purchasers of IT because of the

---

<sup>3</sup> Publictechnology.net & Gartner, Global ICT Public Sector Spend Outstrips Market (Aug. 19, 2010), available at [www.publictechnology.net](http://www.publictechnology.net).

government's deeper involvement in the economy and because governments in these markets are often relatively more intensive IT users.

Increasingly, however, governments in emerging economies are manipulating their procurement rules to exclude foreign products and suppliers. In **China**, the government has introduced a broad array of "indigenous innovation" policies at various levels of government (central, provincial, and municipal). Under one such policy, the Chinese government proposed to develop catalogs of "indigenous innovation" products to receive preferential treatment in procurement, and one of the requirements for becoming listed in the catalogs was that the product's IP was owned and developed in China. Although Chinese leaders have committed in recent bilateral negotiations with the United States to "delink" government procurement from these "innovation" policies, multinational IT suppliers continue to confront this form of discrimination by government agencies at all levels.

Likewise, **India** and **Brazil** have recently taken steps to extend extensive procurement preferences to domestic products and suppliers (see Case Studies A & B, below). **Indonesia** grants procurement preferences designed to maximize the use of local content and encourage domestic sourcing of supplies (see Case Study C, below).

In addition, some emerging markets have pursued measures to mandate or provide significant preferences for procurement of particular technologies. For example, **Brazil** has pursued numerous efforts over the past decade to enact preferences at the federal, state, and local government levels for the procurement of open-source software over commercial products. Most recently, in December 2011, two Brazilian legislative committees approved draft Law PL 2269/1999, which would require all Brazilian federal government agencies and state backed companies to favor open-source software in their procurement policies. This legislation is pending further action in the Brazilian Congress. In **India**, the Department of Higher Education recently circulated a draft information and communications technology (ICT) policy that includes a strong preference for the open-source software licensing model.

Software today often contains a mix of open-source and proprietary elements. Efforts by governments to prescribe one model over another for procurement undermine competition in the marketplace and restrict the ability of government purchasers to procure the best products to meet their needs. In the United States, the White House has reaffirmed its policy of technology neutrality in IT procurement.<sup>4</sup> Similarly, the EU's public procurement law contains an obligation that procurement be nondiscriminatory.<sup>5</sup>

A related and troubling development is the expansion of government procurement restrictions beyond purchases made by government agencies. Many of **China's** procurement preferences appear to cover procurement by state-owned enterprises, a massive sector in China. This is inconsistent with China's efforts to join the WTO Government Procurement

---

<sup>4</sup> Executive Office of the President, Office of Management and Budget, Memorandum for Chief Information Officers and Senior Procurement Executives (Jan. 7, 2011).

<sup>5</sup> Article 23, Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts, and public service contracts.

Agreement (GPA) and with its existing WTO commitment that the government “would not influence, directly or indirectly, commercial decisions on the part of state-owned or state-invested enterprises, including the quantity, value or country of origin of any goods purchased or sold...”<sup>6</sup> The new directive in **India** providing preferences for the procurement of domestically manufactured electronic goods would apply beyond government agencies to procurement by state-licensed entities such as telecommunications service providers (see Case Study A, below).

*Case Study A: Mandates for Procurement of Domestic Electronic Goods in **India***

In February 2012, the Indian government issued a notification implementing procurement mandates for domestically manufactured electronic goods. Under this policy, at least 30 percent of procurements are set aside for domestically manufactured products, which are defined as products with a specified percentage of domestic value-add (starting at 25 percent in the first year and increasing to 45 percent after five years). These preferences apply to procurement by government agencies and to procurement by government-licensed entities such as telecommunications service providers and financial services firms. While the full scope of this policy is still unclear, particularly the extent to which it applies to private entities, it represents a highly restrictive policy that could be expanded to a broader range of IT products and services.

The procurement policy for domestically manufactured electronic goods follows the release by the Ministry of ICT in October 2011 of three draft interrelated national policy initiatives — the National IT Policy, National Telecom Policy, and National Electronics Policy — to promote the development of ICT industries in India. While these policies seek the laudable goal of enhancing India’s ICT sectors, they set a framework for enacting measures to exclude foreign suppliers or impose burdensome requirements on them.

*Case Study B: Price Preferences for Procurement of Local Goods in **Brazil***

In late 2010, the Brazilian government enacted a law that imposed sweeping new government procurement preferences for local products.

Law 12.349/2010 gives preference in public tenders to bidders that offer goods and services that are produced in Brazil and are fully compliant with Brazilian technical standards and regulations. The extent of the preference depends on the industry, but the law allows a preference margin of up to 25 percent of the price of foreign-origin products and services. The preference may be adjusted depending on studies that establish criteria for how best to generate jobs and innovation in Brazil. In addition, the law allows for procurement of “strategic” ICT goods and services to be restricted to those with indigenously developed technology.

Recently, the Brazilian Ministry of Science, Technology & Innovation (MCTI) released a “Bigger IT Plan” to bolster the growth of the domestic IT industry. The program focuses

---

<sup>6</sup> WTO, Working Party on the Accession of China — Report of the Working Party on the Accession of China, 46 (Oct. 1, 2011).

heavily on software and related services and includes a new process for the government to evaluate and certify that software products are locally developed in order to qualify for the government procurement price preferences that could be as high as 25 percent.

*Case Study C: Central and State-Level Procurement Preferences in Indonesia*

Indonesia has issued a series of policies aimed at maximizing procurement of local products for both central- and state-level government entities. Presidential Regulation 54/2010 calls for procuring entities to maximize local content in procurement, use foreign components only when necessary, and designate foreign contractors as subcontractors to local companies. Presidential Regulation 2/2009 calls on state administrations to optimize the use of domestic goods and services and give price preferences for domestic goods and providers. Ministry of Industry Decree (15/2011) establishes an Accelerated Use of Local Product National Team to optimize procurement of local goods and services.

## **2. Manipulation of Technology Standards**

Technology standards play a vital role in facilitating global trade in IT products and services. 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.

IT companies invest substantial resources to develop and support technology standards that can be used globally and to make them available for licensing on fair, reasonable, and nondiscriminatory (FRAND) terms to companies large and small, regardless of nationality. This process has generated enormous benefits for consumers. Not only has it spurred technology innovation, but experience has shown that standards are most successful when developed in market-led, voluntary, and consensus-based processes. Discriminatory government-mandated standards, by contrast, tend to “freeze” innovation and force consumers and businesses into using products that might not suit their needs.

Nonetheless, we are seeing governments manipulating standard-setting processes in an effort to bolster domestic firms and insulate them from foreign competition.

In **China**, regulators have pressed domestic standards development organizations (SDOs) to adopt standards put forward by domestic firms or that implement patented technologies owned by these firms over more widely adopted international standards (See Case Study D, below). As part of its “indigenous innovation” efforts, China has adopted or sought to develop unique Chinese standards in areas including, among others, Internet protocols, 3G telecommunications services, wireless local area networks, digital audio and video, radio frequency identification technology, and encryption.

Chinese SDOs also may restrict meaningful foreign participation, which can make it difficult for non-Chinese entities to influence standards development or protect their patents. Separately, China's rules for testing and certifying compliance with standards are often discriminatory and unduly burdensome and provide inadequate protections for confidential commercial information (including software source code) and intellectual property rights.

**India** has adopted policies that favor domestic standards and technologies and discourage compensating patent holders for technologies that are essential to standards (see Case Study E, below).

*Case Study D: Restrictive Standards Policies and Practices in China*

In 2005, China articulated a National Standards Policy to modernize its standards regime. As a result of this policy and further regulations issued in January 2010 (the Disposal Rules for Inclusion of Patents in National Standards), China's Standardization Administration gained authority over a number of Chinese standards development organizations (SDOs). Although the regulations state that, in principle, foreign firms are allowed to participate fully in such committees, there have been reports of SDOs excluding foreign firms from meetings or preventing them from participating in meaningful ways, which in some cases has led to the "capture" of Chinese standards by Chinese domestic firms. Moreover, in order to participate in standard-setting, foreign firms may be required to disclose confidential and proprietary information, including patented technologies, without assurances that such information will be protected.

For example, the Ministry of Industry and Information Technology is developing standards for software asset management, which already has an International Organization for Standardization (ISO) standard. Foreign companies, which have a wealth of information on global software asset management practices, cannot fully participate in this standard development process.

In addition, China's Standardization Administration does not recognize standards developed by highly reputable, industry-led SDOs such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). Instead, it recognizes standards only if they are developed by China's standard-setting committees or a select few others.

*Case Study E: Unreasonable Terms for Standards-Essential Patents and Preferences for Indigenous Technology in India*

In November 2010, the Indian government announced a policy on open standards for e-governance. The goal of the policy is for standards-essential patents to be made available on a royalty-free basis rather than on fair, reasonable, and nondiscriminatory terms (FRAND). This denies patent holders suitable compensation for their intellectual property and dissuades them from participating in standard-setting processes.

Separately, India's National Telecom Policy takes steps to promote new Indian standards for use in the telecommunications industry. It calls for the establishment of a new

Telecommunications Standard Development Organization to aid the development of new Indian standards and promote the use of Indian standards internationally. The Telecom Policy encourages the use of local standards to protect national security and specifically promotes Indian-origin SIM cards that are designed to incorporate Indian standards.

### 3. Overreaching Security-Related Regulations

Under the guise of protecting national security, implementing stronger cyber-security measures, or otherwise improving “security,” emerging-market governments are imposing measures that often stray far into the commercial sphere. These include procurement restrictions or unreasonable testing and certification requirements. These measures and others create barriers for foreign IT products and deny local consumers and businesses access to the best security solutions to meet their needs. In some instances, these measures actually undermine security.

For example, **China’s** Multi-Level Protection Scheme (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 (see Case Study F, below). **India** imposes costly and burdensome in-country testing and certification requirements on products procured by telecommunications service providers (see Case Study G, below). **Russia** has licensing requirements for imports of products with encryption technology that has the effect of delaying and impeding imports.

#### Case Study F: Restrictions on the Procurement of Foreign IT Security Products in **China**

IT suppliers face a significant security-related market barrier in China’s Multi-Level Protection Scheme (MLPS), which classifies information networks in China based on their relative importance to national security, social order, and economic interests. Any information system classified as level three or higher on a scale of one to five is subject to certain restrictions that have the effect of excluding foreign technologies and firms.

For example, only companies owned by Chinese citizens are allowed to supply IT security products for these systems, and the core technology and key components of the products must contain domestic IP.

Because of the broad and nonspecific language used to describe the different classification levels, most of China’s large state-owned enterprises and government agencies in the areas of finance, transportation, telecommunications, health, education, and other areas not directly related to security are classified at level three or higher. China’s Ministry of Public Security began sending out inspectors in summer 2010 to identify violators. The inspection campaign aims to achieve “full compliance” among systems classified at level three or above in 2012. To satisfy the MLPS requirements, many state-owned enterprises that once procured foreign IT security products have switched to domestic products.

### Case Study G: Burdensome Security Testing for IT Products in India

In December 2009, India's Department of Telecommunications issued a series of new rules for telecommunications service providers (TSPs) that required hardware and software vendors to transfer technology and escrow source code and other sensitive design elements with the TSPs. These requirements, which were announced as a means of improving the security of India's commercial telecom networks, applied only to imported products. The policy eventually was amended to eliminate the technology transfer and source code escrow requirements, but it still imposes significant burdens on foreign firms.

Beginning April 1, 2013, all network "elements" must be tested and certified by authorized laboratories in India. That will preclude companies from utilizing long-established, internationally accredited laboratories in other countries. The in-country testing and certification is required even though there is no evidence that where the test is performed has any bearing on its accuracy as long as the laboratory has achieved appropriate accreditation.

The new requirements also have a mandatory facility inspection provision. The TSP must ensure that it, the Department of Telecommunications, or other designated agencies are allowed to inspect vendors' "hardware, software, design, development, manufacturing facility, and supply chain" and "subject all software to a security/threat check" at any time while the vendor is supplying equipment to the TSP. These new inspection requirements will impose a barrier on foreign IT companies' ability to sell to Indian telecommunications operators because most of the foreign suppliers' facilities are located outside India, making compliance more costly and cumbersome than for their in-country competitors.

#### **4. Regulatory Obstacles 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. But to fully seize the economic opportunity that cloud computing offers, it is critical to remove regulatory obstacles sprouting up in many key markets.

A recent study found that IT innovations enabled by the cloud could generate increased business revenue of \$1.1 trillion a year by 2015 and that spending on public and private IT cloud services would generate nearly 14 million jobs worldwide from 2011 to 2015.<sup>7</sup> Notably, more than 50 percent of the new jobs created would be for small- and medium-sized businesses. Job growth linked to cloud computing will be spread globally, with nearly 1.2 million jobs created in the United States and Canada and 6.75 million jobs in China and India by the end of 2015.

---

<sup>7</sup> IDC, Cloud Computing's Role in Job Creation (March 2012), available at [http://www.microsoft.com/en-us/news/download/features/2012/IDC\\_Cloud\\_jobs\\_White\\_Paper.pdf](http://www.microsoft.com/en-us/news/download/features/2012/IDC_Cloud_jobs_White_Paper.pdf).

Many governments, recognizing the potential economic opportunity, are reviewing their regulatory regimes to ensure they are cloud-ready and are working to eliminate rules that unnecessarily impede cloud services. In the United States, for example, the Federal government's Chief Information Officer released a *Federal Cloud Computing Strategy* in 2011. That effort includes a "Cloud First" approach intended to promote the use of cloud technologies.<sup>8</sup>

Rules restricting the free flow of data 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.

While efforts are under way in some markets to ease the flow of data among jurisdictions, other governments have taken a different path. For example, **Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Costa Rica, Greece, Hong Kong, India, Indonesia, Korea, Mexico, Peru, Russia, Switzerland, and Vietnam**, all have adopted or proposed rules that prohibit or significantly restrict companies from transferring personal information out of the domestic territory. In some cases, markets are requiring that data centers be located inside their geographic borders.

Policies that unnecessarily restrict the free flow of data 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 datacenter or national network fails.

In some markets, licensing rules have created significant obstacles to the entry of foreign cloud providers. For example, because appropriate licenses are available to foreign firms only in certain narrow circumstances, the cloud market in **China** is largely closed to foreign competition (see Case Study H, below).

Moreover, US companies face a significant barrier to conducting cloud computing and other internet-based business in **China** due to Chinese policies that block or significantly delay access to services hosted outside China. China's "Great Firewall" 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. The Great Firewall has impacted a broad range of cross-border Internet traffic, including business-to-business services that are legal in China and for which there appears to be no justification under WTO services rules. The operation of the Great Firewall prevents many US companies from reliably selling or delivering cloud computing services into the Chinese

---

<sup>8</sup> Vivek Kundra, White House, Federal Cloud Computing Strategy (Feb. 8, 2011).

market from servers hosted outside of China and greatly undermines their business prospects. We are pleased that USTR has raised concerns about this with Chinese officials and asked them for detailed information about when and how such restrictions are implemented with an eye toward assessing whether these practices violate China's WTO commitments.

Subpar privacy rules also create an obstacle to market access for cloud providers. Users will migrate to the cloud only if they have confidence that their data will be safe there. Accordingly, national privacy regimes should be predictable and transparent and should avoid unnecessarily burdensome restrictions on cloud service providers such as registration requirements for data controllers and cross-border data transfers. Cloud providers should be encouraged to establish privacy policies that are appropriate for the particular cloud service they provide and the business model they use. Key emerging markets for cloud services, including **China, India, Indonesia, Thailand, and Turkey**, do not yet have adequate data protection laws in place, although such laws are currently under consideration in several of these markets.

Earlier this year, BSA released its Global Cloud Computing Scorecard, a comprehensive assessment of the cloud "readiness" of 24 global markets. 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. This submission draws on information available in that report. The report, along with detailed reviews of the legal and regulatory frameworks in the countries analyzed, is available at [www.bsa.org/cloudscorecard](http://www.bsa.org/cloudscorecard).

Specific examples of these regulatory obstacles to cloud computing include:

- **Canada, China, Greece, India, and Malaysia**, which have data residency laws that require companies to store data on servers located in the country where it is collected;
- **Korea**, which is considering restrictions that would prevent insurers from transferring data outside the country, despite provisions in the recent KORUS Free Trade Agreement designed to allow the use of regional data processing hubs;
- **Korea**, which is now considering a "Bill on the Development of Cloud Computing and Protection of its Users" that threatens to present several obstacles for international cloud computing providers by imposing strict regulatory requirements and potentially requiring new Korea-specific standards;
- **Indonesia**, where the government in August 2011 issued a draft amendment that would require data service providers to establish local representation in Indonesia, including local data centers; and
- **Vietnam**, where the Ministry of Information and Communication issued a draft decree that would impose a number of new licensing and registration requirements on IT services and subject providers of data center and cloud computing services to significant restrictions on the cross-border supply of services and requirements that they locate entire equipment systems used for providing such services in the country.

### Case Study H: Licensing Requirements Restricting Foreign Companies' Ability to Offer Cloud Services in China

In China, entities wishing to provide value-added telecommunication services (“VATS”) are required to have a VATS license. A particular type of VATS license, known as an ICP license, is required to provide commercial Internet content services, including any Web- or cloud-based content services.

VATS licenses are subject to strict regulation and approval by the Ministry of Industry and Information Technology (MIIT) and several other government authorities. With the exception of a specific type of joint venture known as a foreign invested telecommunications enterprise (FITE), foreign invested companies are not eligible to apply for a VATS license (including an ICP license). Because of the strict regulatory requirements for FITEs — for example, foreign investment in the FITE must not exceed 50 percent of the enterprise’s equity interest, the registered capital must be at least RMB 10 million (\$1.6 million) if the FITE will engage in nationwide or interprovincial services, and the foreign investor must prove that it has successful experience in providing value-added telecommunication services in the relevant field — it is difficult to obtain approval from MIIT to establish a FITE. Moreover, MIIT has specified that the places and facilities necessary to operate the services must be “installed within the coverage scope as prescribed by the Business License,” which is generally understood to mean that any servers and data centers used to support cloud services must be located in China. MIIT has reportedly not issued a single ICP license to a foreign enterprise in the past two to three years.

The VATS/ICP requirements have forced foreign companies to consider less attractive and often unworkable alternatives. For example, some foreign cloud providers are entering into licensing arrangements under which the foreign company provides Web services in China through a contractual licensing relationship with a local agent that already holds an ICP license. This licensing model has inherent IP risks, because the foreign company may need to transfer sensitive IP to the Chinese company while having little control over the management and operation of the Web services provided by the local company. Furthermore, cross-border technology license arrangements are subject to the requirements of China’s Technology Import and Export Regulations. Under these regulations, the foreign company must guarantee that the licensed technology is complete, accurate, effective, and capable of achieving the agreed technical objectives, and the foreign company is obliged to defend and indemnify the Chinese party against any claim that the technology infringes third-party rights. Meanwhile, because the foreign party is prohibited from placing restrictions upon the Chinese party regarding improvements to the technology, the Chinese party is free to develop derivative works based on the licensed technology and claim the derivative works as its own.

## **5. Persistent Tariffs on IT Products**

The multilateral Information Technology Agreement (ITA), launched in 1996 under the auspices of the WTO, has had an enormous impact on removing tariff barriers to global trade in IT products. The signatory countries to the ITA agreed to lower tariff barriers on a wide

array of IT products. According to a recent report, implementation of the ITA was a key driver in the expansion of global trade in information and communications technology products from \$1.2 trillion in 1996 to \$4 trillion in 2008.<sup>9</sup>

The ITA, however, has not kept pace with IT product development. In the years since the ITA was inaugurated, global IT companies have come out with a broad array of products that are not covered under the agreement, including new types of semiconductor chips, IT-enabled medical devices, and such computer accessories as monitors and speakers, DVD players, and video game consoles. By not keeping pace with technological developments, the ITA does not cover many products that are vital to the business plans of IT companies today. By some estimates, an expanded ITA could remove tariffs on \$800 billion or more of global information and communications technology trade.<sup>10</sup>

Moreover, while today there are more than 70 signatory countries to the ITA, several important economies are not members, including Brazil, Chile, and Russia (which recently joined the WTO, but to date has not joined the ITA). The lack of participation in the ITA by these critical markets for IT products is significantly hampering the ability of global companies to sell IT products there and closing off consumers in these countries to products that can enhance their productivity and well-being.

We strongly support the efforts underway by the United States and several other members of the ITA to begin talks toward expanding the agreement and hope to see these discussions move forward expeditiously in the coming months.

---

<sup>9</sup> Information Technology and Innovation Foundation, *Boosting Exports, Jobs, and Economic Growth by Expanding the ITA*, at 1 (March 2012), available at [www.itif.org](http://www.itif.org).

<sup>10</sup> Information Technology and Innovation Foundation, *Boosting Exports, Jobs, and Economic Growth by Expanding the ITA*, at 2.