SPECIAL 301 SUBMISSION

February 6, 2015

Docket No. USTR-2014-0025
Susan F. Wilson
Director for Intellectual Property and Innovation,
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Ms. Wilson,

BSA | The Software Alliance[1] provides the following information pursuant to your request for written submissions on whether US trading partners should be designated Priority Foreign Country, Priority Watch List or Watch List in the 2015 Special 301 Report.

Pursuant to the Special 301 statutory mandate, Section 182 of the Trade Act of 1974, as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreements Act of 1994 (19 USC § 2242), requires USTR to identify "those foreign countries that **deny adequate and effective protection of intellectual property rights**, ***or*** **deny fair and equitable market access to United States persons that rely upon intellectual property protection**" (emphasis added).

In this submission, we address both elements of Section 182 of the Trade Act. The report describes US trading partners with **deficiencies in protecting and enforcing intellectual property rights** *and* US trading partners that have erected **unfair market access barriers** to BSA member software, computer and technology products and services. In many cases, US

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Altium, Apple, ANSYS, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, Parallels, PTC, salesforce.com, Siemens PLM, Symantec, Tekla, The MathWorks, and Trend Micro.

20 F Street NW, Suite 800
Washington, DC 20011
P 202-872-5500
W bsa.org

trading partners are deficient on both counts. For some countries, the market access barriers present the higher threat to BSA members' ability to do business in the market.

BSA members develop innovative software solutions and invest substantial resources into developing cutting edge technologies that are at the forefront of driving the global digital economy.

In the past, BSA has filed our Special 301 submissions jointly with other copyright-intensive industries but for the reasons state below, we are filing this submission to highlight the challenges faced by software and technology.

Adequate **copyright** protection and enforcement remains a critical element for a successful commercial environment in US trading partners for BSA members. But the protection and enforcement of other forms of intellectual property, such as **patents and trade secrets**, are equally important to BSA members. In addition, eliminating **market access barriers** that US trading partners erect that discriminate against or impede BSA members in overseas markets is also critical for the continued health and growth of the software and information and communications technology (ICT) sector.

BSA members, like the other copyright-intensive industries, face significant challenges due to the availability of extensive use of unlicensed copies of works. But BSA's primary enforcement challenge, and the main intellectual property-related threat to our ability to participate in overseas markets effectively, is the use of **unlicensed** software products or services **by governments, state-owned enterprises (SOEs) and business entities.**

In the following sections, BSA provides country reports on US trading partners to express our concerns about the extent to which these countries provide **fair and equitable market access** to BSA members, or provide **adequate and effective enforcement of intellectual property**, or both. We recommend these countries to be listed on USTR's Priority Watch List or Watch List. We also list a number of Countries of Concern: markets where we have on-going concerns regarding these matters but for which we are not explicitly requesting listing in USTR's Special 301 Report as Watch List, Priority Watch List, or Priority Foreign Countries.

Priority Watch List:	**Argentina, Chile, China, India, Indonesia, Russia, and Vietnam**
Watch List:	**Brazil, Bulgaria, Greece, Kazakhstan, Korea, Mexico, South Africa, Thailand, and Turkey**
Countries of Concern:	**Azerbaijan, Malaysia, Moldova, Nigeria, the Philippines, Romania, Saudi Arabia, and Spain**

The country reports immediately following this introduction to our submission lay out BSA's specific concerns related to intellectual property protection and market access barriers in each of the countries cited. BSA can provide additional information with respect to each market as need.

Market Access

Cross-border data flows: The free flow of data across borders will be a key pillar of economic growth in the 21st century. This can be linked to two interconnected trends. First, more and more economic activity is moving to, or being born on, the Internet and, at the same time, the cost of online data collection, storage, and processing has continued to plummet. Likewise, the software industry itself is undergoing a dramatic transformation, with companies adjusting their business models so that software is increasingly offered as a subscription service enabled through the transfer of data online. The transfer of data across borders is critical to both the business offerings and core operations of enterprises that make up the digital economy. A number of countries, including **Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Costa Rica, Greece, Hong Kong, India, Indonesia, South Korea, Mexico, Nigeria, Peru, Russia, Switzerland and Vietnam**, have adopted or have proposed rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory. In many instances these are outright prohibitions, while in others they are requirements that data from its citizens be stored and processed only within the country's territory.

Procurement Discrimination: Governments are among the biggest consumers of ICT products and services. Yet many are imposing significant restrictions on foreign suppliers' ability to serve public-sector customers. Not only do such policies eliminate potential sales for BSA members, but they also deny government purchasers the freedom to choose the best available products and services to meet their needs. US trading partners with existing or proposed restrictions against public procurement for foreign ICT products and services include **Brazil, China, Germany, India, South Korea, Nigeria, Russia, Taiwan, the United Kingdom, and Vietnam.**

Security: Governments around the world have a legitimate interest in ensuring that the ICT equipment, software and services deployed in their countries are reliable, safe and secure. However, a number of countries are using or proposing to use security concerns to justify *de facto* trade barriers. Such countries include **Brazil, China, France, Germany, India, Indonesia, Japan, South Korea, Nigeria, Russia, and Vietnam**.

Standards: Technology standards play a vital role in facilitating global trade in information technologies. When standards are developed through voluntary, industry-led processes, and widely used across markets, they generate efficiencies of scale and speed the development and distribution on innovative products and services. Unfortunately, a number of countries have developed or are developing country-specific standards to favor local companies and protect them against foreign competition. This creates a *de facto* trade barrier for BSA members, raises the costs of cutting edge technologies to consumers and enterprises, and places the domestic firms

these policies are designed to protect at a disadvantage in the global market place. Countries adopting nationalized standards for ICT products include **Brazil, China, India, Nigeria, and Vietnam**.

Intellectual Property

Patents: BSA members invest enormous resources to develop cutting edge technologies and software-enabled solutions for business, governments and consumers. It is therefore critical that countries provide effective patent protection to eligible computer-implemented inventions, in line with their international obligations. Unfortunately, a number of countries have established or are considering policies that make obtaining patent protection for such inventions impossible or difficult. Such countries include **Brazil, India, and Thailand**, among others.

Some countries have adopted or are considering policies that could significantly constrain the freedom of patent holders to freely negotiate licenses for their inventions. For example, **China** has proposed a variety of policies that could unfairly restrict the ability of patent holders to exercise their legitimate rights to enforce their patents or to negotiate mutually acceptable licensing terms. **China** has also proposed rules that would constrain the ability of innovative companies conducting research and development in China to establish company policies or negotiate employee contracts regarding the ownership and remuneration of inventions created by employee-inventors in the course of their employment duties.

Trade Secrets: BSA members also rely on the ability to protect valuable trade secrets and other proprietary information to maintain their competitive position in the global market place. US trading partners that fail to implement and enforce strong rules protecting trade secrets against misappropriation or unauthorized disclosure put BSA members' business operations at risk and prevent them from having legal recourse when misappropriation or unauthorized disclosure occurs. Given the ease by which such information can be transmitted, this presents serious market challenges not only in the particular country in question, but globally as well. Policies in place or proposed to require the disclosure of sensitive information as a condition for market access represent enormous market access barriers for BSA members. Countries with or proposing such policies include **China, Indonesia, Nigeria, and Russia.**

License Compliance/Illicit Use of Software: The use of unlicensed software by enterprises and governments is one of the major commercial challenges for BSA members. According to the latest information, the commercial value of unlicensed software globally is at least US$62 billion, a staggering sum.[2] Not only does unlicensed use of software impact the revenue stream of BSA

[2] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

members, deterring investments in further innovation, but also the use of unlicensed software also exposes enterprises and agencies engaged in such activity to higher risks of malware infections and other security vulnerabilities.[3]

BSA has engaged with US trading partners in an effort to reduce the incidence of unlicensed software use by enterprises and government entities, with varying degrees of success. These efforts include promoting voluntary compliance measures, such as promoting effective, transparent and verifiable software asset management (SAM) procedures, where enterprises and government agencies conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed. BSA has developed the Verafirm Certification program, which confirms that an organization's SAM practices are aligned with the ISO19770-1 SAM standard. Governments can lead by example and adopt such measures for their own procurement and IT maintenance systems, which can send a powerful example to enterprises in their companies. **Mexico** has been a leader in this regard.

Voluntary measures are only part of the solution. In order to have a meaningful impact on reducing the use of unlicensed software, US trading partners must adopt and enforce effective legal mechanisms by which BSA members can enforce their rights and compel licensing compliance. The legal mechanisms need to be efficient, without overly burdensome procedures or undue delays, and must result in penalties or damages that are sufficient to compensate the rights holder and deter future infringements.

BSA remains highly concerned about the inadequacy of enforcement in a wide variety of countries. Often this is the result of deficiencies in the legislative framework. In addition to the countries explicitly cited in this submission, examples of countries where the laws do not provide adequate legal protection to enforce against enterprises that use unlicensed software in the course of their commercial activities include **Armenia, Belarus, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan.**

Regardless of the quality, or lack thereof, of the underlying legal framework, if the authorities are unable or unwilling to enforce the law, BSA members are unable to receive adequate protection and enforcement of their intellectual property rights. In addition to the countries explicitly citied in this submission, examples of countries that fail to provide adequate enforcement of BSA members' intellectual property rights include **Armenia, Croatia, Kyrgyzstan, Macedonia, and Qatar.**

Government and SOE Legalization: Unlicensed use by governments of software is particularly challenging to BSA members. Because these are the entities upon which BSA members rely to provide protection and enforcement of their intellectual property rights, if the governments themselves are unwilling to comply with the law there is often little that BSA or our members can

[3] For example, see "Unlicensed Software and Cyber Security Threats", IDC 2014 available at http://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf.

do on our own. We urge the US government to aggressively engage with US trading partners on behalf of US companies' rights and interests.

Some governments, like **Mexico**, have taken laudable steps to establish mechanisms within government agencies to ensure that only licensed software is purchased and used. Other governments have made commitments to ensure licensing compliance in government agencies and government funded entities, including SOEs. Despites commitments to the United States under the US-Korea Free Trade Agreement (KORUS FTA)[4], some government agencies in **South Korea** continue to under-license the software they use. **China** has made multiple commitments to the United State in bilateral fora such as the Joint Commission on Commerce and Trade (JCCT) and the Strategic and Economic Dialogue (S&ED) to ensure the legal use of software by government agencies and SOEs. Unfortunately, to date the **China** has failed to implement effective, transparent and verifiable software asset management procedures to ensure and maintain actual legal use of software by government agencies and SOEs. Although **Taiwan** established a new "Software Procurement Office" in mid-2014 to create a platform that consolidates and centralizes software bidding and procurement processes, no meaningful progress has been made in developing an overall software asset management mechanism for government agencies. As a result, the risk of using under-licensed software remains significant in certain government agencies. Substantial efforts to escalate the use of unlicensed or under-licensed software in government agencies in **Macedonia** have not led to any meaningful progress on the matter.

In April 2013, USTR designated **Ukraine** as a Priority Foreign Country due to, among other things, widespread use of unlicensed software by government agencies. **Ukraine** had made commitments to take steps that are "necessary to transition government ministries to licensed software, to include training for inspectors, as well as ongoing technical assistance to each Ministry in setting up an internal monitoring and compliance system." At the time of USTR's designation of **Ukraine** as a Priority Foreign Country, however, **Ukraine** had not allocated necessary resources and had failed to make any meaningful progress on this matter. In February 2014, USTR "determined that certain intellectual property rights (IPR) acts, policies, and practices of **Ukraine** are unreasonable and burden or restrict United States commerce and are thus actionable under section 301(b) of the Trade Act of 1974, as amended." In light of the political situation in **Ukraine** at that time, USTR determined that "no action under section 301 is appropriate at this time." There has been no change or improvement in the intellectual property situation since USTR made this determination.

BSA recognizes that the political situation in **Ukraine** remains severe. We hope that the internal situation and **Ukraine's** relations with its neighbors will normalize soon. As the United States reengages in a comprehensive economic dialogue with **Ukraine**, BSA urges the US government to ensure that **Ukraine** follows through with its past commitments to ensure that government

[4] US-Korea Free Trade Agreement – Article 18.4(9), available at https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file273_12717.pdf.

agencies are using only licensed software. BSA looks forward to working the governments of the United States and **Ukraine** to develop a meaningful action plan to quickly address these long-standing concerns.

Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the 2015 Special 301 Report and the US government's engagement with important trading partners in 2015. We look forward to working with USTR and the US agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee to achieve meaningful progress in ensuring that BSA members and others that rely on intellectual property receive **fair and equitable market access** to important US trading partners and **adequate and effective protection and enforcement of their intellectual property rights.**

Table of Contents

	Page #
Priority Watch List ……	**9**
Argentina ……	**10**
Chile ……	**12**
China ……...	**14**
India …….	**22**
Indonesia …….	**26**
Russia ……..	**29**
Vietnam ……...	**32**
Watch List ……	**36**
Brazil ……...	**37**
Bulgaria ……...	**41**
Greece ……..	**43**
Kazakhstan ……	**45**
Korea, Republic of …….	**47**
Mexico …….	**51**
South Africa ……	**53**
Thailand ……..	**55**
Turkey …….	**58**
Countries of Concern ……..	**60**
Azerbaijan ……...	**61**
Malaysia ……..	**62**
Moldova ……...	**65**
Nigeria …….	**66**
the Philippines ……	**68**
Romania ……..	**70**
Saudi Arabia ……...	**72**
Spain ……	**74**

Priority Watch List

ARGENTINA

Due to sustained high levels of unlicensed software use by enterprises, a lack of political commitment to make necessary changes to the legislative framework, and severe barriers to doing business in-country, BSA recommends that Argentina remain on the Priority Watch List.

Overview/Business Environment

The business environment in Argentina for BSA members is very challenging, and in 2014 it deteriorated as a result of monetary policies and an overall declining economic environment. There is little political will to elevate the importance of the protection and enforcement of intellectual property, and law enforcement authorities do not consider intellectual property infringements a priority.

Market Access

Due to broader economic circumstances, the government has imposed severe currency exchange restrictions, prohibiting the payment of dividends and royalties to foreign parties. This, in turn, makes it difficult for Argentinian enterprises that seek proper licenses for their software to obtain the currency needed to pay for those licenses. This is a severe challenge to BSA members doing business in Argentina.

BSA has previously noted a problem with tax policy in Argentina. Argentina's Customs and Tax Authority (the Administración Federal de Ingresos Públicos, or AFIP) refuses to apply the special rules that the Income Tax Act provides for "authors' rights" international transfers. AFIP contends that the legal nomenclature "author" is limited to physical persons, and that a legal person (e.g., a corporation) cannot be an author and, as a result, cannot hold these "authors rights." This problem could be solved by amending the Income Tax Act to establish a concrete withholding rate for software license payments, similar to what was done several years ago for music and motion pictures. There is also a clear need for the United States and Argentina to reach agreement on a treaty to avoid double taxation. The difficulty of obtaining foreign currency, however, has superseded these tax issues at present.

Copyright and Enforcement

According to the most recent data, the rate of unlicensed software use in Argentina remains static at 69 percent in 2013, significantly higher that the regional average. This represents a commercial value of US$950 million in unlicensed software.[1]

Enterprise Licensing/Legalization: Enterprise use of unlicensed software remains a significant challenge, especially for small- and medium-sized companies. The changes are even more acute in certain provinces of lesser economic development.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Government Licensing/Legalization: With respect to government legalization efforts, the software industry continues to seek from the Argentine government (in particular, the Subsecretaría de la Gestión Pública – the Undersecretariat for Public Administration) an executive decree that would mandate legal software use in government agencies. The decree should also require government agencies to implement verifiable software asset management procedures, where government agencies conduct audits of the software they have installed to ensure, among other things, that all copies in use are properly licensed. While several "standards" have been issued by the Subsecretaría, the Argentine government, these have not been effective at addressing the continued use of unlicensed software in government agencies.

Statutory and Regulatory Provisions: BSA members have identified the following important elements that would benefit from clarifications or express incorporation in the copyright law:

- Extend the scope of the reproduction right to explicitly cover temporary copies;
- Protect against the act of circumvention as well as the manufacture or distribution of devices aimed at circumventing technological protection measures (TPMs);
- Establish effective statutory damages provisions in civil infringement cases; and
- Recognize intellectual property ownership by legal entities on the same footing with natural personas to comport with international practice.

Compliance and Enforcement: BSA engages only in civil actions in Argentina. In general terms, provisional injunctions are available and are one of the most favorable characteristics of the domestic system. BSA brought 112 cases in 2014 we currently have approximately 100 cases currently pending in the courts of Buenos Aires and neighboring jurisdictions.

The criminal system is not an effective tool for enforcement against unlicensed use of software by enterprises. Intellectual property is not a priority for prosecutors and effective remedies are not available. Similarly, intellectual property enforcement is not a priority for customs authorities.

Technical Assistance and Education: The local information and communication technology (ICT) sector engages in constant activity to support promoting and updating Argentinian legislation aimed to benefit creative industries.

On May 8, 2014, with the cooperation of Buenos Aires Autonomous City government and a number of sponsors, Fundación Clementina, with the principal sponsorship of BSA organized a roundtable on updating and optimization intellectual property law. Key representatives of creative industries participated, as well as a representative of the governing party and a minister of the local government. We plan to repeat the effort during the first part of 2015.

Recommendation: Due to sustained high levels of unlicensed software use by enterprises, a lack of political commitment to make necessary changes to the legislative framework, and severe barriers to doing business in-country, BSA recommends that Argentina remain on the **Priority Watch List**.

CHILE

Due to on-going challenges in enforcing against unlicensed software use by enterprises and Chile's failure to make meaningful progress in improving its laws and policies, BSA recommends that USTR maintain Chile on the Priority Watch List.

Overview/Business Environment

The overall business environment for software in Chile remained largely unchanged in 2014. According to the most recent data, the rate of unlicensed software Chile has dropped only marginally from 61 percent in 2011 to 59 percent in 2013. This represents a commercial value of US$378 million in unlicensed software.[1]

The new government which took office on March 11 has not issued any policy changes to specifically address unlicensed use of software. Inadequacies in the law remain unaddressed and remedies for unlicensed use remain inadequate.

Copyright and Enforcement

The fundamental issue of concern for BSA members in Chile is the very high rate of unlicensed use of software by enterprises and the absence of meaningful actions by the government to address the problem.

***Enterprise Licensing/Legalization*:** Most service industry sectors, including architecture, design, engineering, and media continue to exhibit high rates of unlicensed software use. Problems also persist with unauthorized pre-installation of software by hardware retailers, and in-house and external providers of information and communication technology (ICT) services that often load unauthorized copies of software onto computers or networks.

Government and SOE Licensing/Legalization: The US-Chile Free Trade Agreement (FTA) obligates the Government of Chile "to actively regulate the acquisition and management of software for such government use."[2] Although there has been progress with government software legalization, more steps are necessary. Establishing and implementing appropriate provisions to regulate the acquisition and management of software by the government is critical to real success. The adoption of effective, transparent, and verifiable software asset management procedures, where government agencies conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed, could also provide a powerful positive example to private enterprises.

Statutory and Regulatory Provisions: The FTA also contains detailed requirements for legal protections against the circumvention of technological protection measures used by BSA members to ensure that only

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[2] United States – Chile Free Trade Agreement Article 17.7.4

licensed users are able to access their software products and services.[3] Chile has still not implemented necessary legislation and regulations to meet its obligations under this provision. As a consequence, in Chile it is easy to obtain illicit activation keys and services that offer the circumvention of technological protection measures.

Compliance and Enforcement: BSA enjoys a good relationship with the Chilean intellectual property agency, INAPI, and with the Director of the Tax Agency. During 2014, BSA conducted almost 70 civil compliance inspections of a variety of enterprises on behalf of our members. We also made more than 150 compliance contacts with companies who should have some level of licensed software, urging them to comply with the law.

In order to conduct civil inspections, civil *ex parte* actions remain a critical remedy for the BSA. Unfortunately, these are hampered by a provision of Chilean law that requires filing *ex parte* search requests in a public electronic register, allowing companies under investigation to learn about a search request before the inspection takes place. This notification requirement can significantly undermine the effectiveness of the search.

Damages awards remain too low to deter users of unlicensed software and there are no provisions for statutory damages. The FTA requires the availability statutory damages.[4]

Recommendation: Due to on-going challenges in enforcing unlicensed software use by enterprises and Chile's failure to make meaningful progress in improving its laws and policies, BSA recommends that USTR maintain Chile on the **Priority Watch List**.

[3] United States – Chile Free Trade Agreement Article 17.7.5

[4] United States – Chile Free Trade Agreement Article 17.11.9

CHINA

Due to continuing high levels of unlicensed software use by enterprises and a deteriorating market access environment for the information and communications technology (ICT) sector, BSA recommends that China be maintained on the Priority Watch List.

Overview/Business Environment

The commercial environment in China for information and communication technology (ICT) generally, and for commercial software in particular, has become more challenging during 2014. For many years, BSA members have struggled against sometimes vague, sometimes explicit indications or instructions from senior Chinese policymakers directing Chinese agencies, Chinese state-owned enterprises (SOEs) and domestic firms generally, to give preference to domestic software. Such measures are often represented as a combination of cost-savings measures and as efforts to promote the domestic software industry.

In 2014, security justifications for procurement preferences and other market access barriers, have become much more common. While BSA members are global leaders in providing secure and reliable software solutions and related technologies to enterprises and consumers, many are concerned that emerging policies could effectively block BSA members and other foreign suppliers from an increasing number of important sectors in the Chinese economy.

In addition to the emerging developments, China's existing regulatory regime makes it extremely difficult for foreign firms to invest in the digital market. There has been no progress in reforming the existing system, which effectively excludes foreign investment in cloud- or other data-services in China. China continues to regulate Internet Services as Value-Added Telecom Services (VATS) and requires licenses that are not available to wholly-owned or majority-owned foreign entities.

These policies, combined with broader "indigenous innovation" policies, contribute to a declining market access environment for many BSA members. This threatens to harm the US-China trade and economic relationship as well as Chinese businesses and consumers.

The intellectual property environment remains extremely challenging. BSA is observing with close interest developments related to copyright reform, patent litigation, proposals to regulate the reward and remuneration of employee-inventors, and policy and legal developments regarding patents involved in standards, among other things. We also remain very interested in meaningful reforms in the protection and enforcement of trade secrets in China, including how sensitive proprietary information that is required by government agencies for regulatory approval purposes is protected.

BSA continues to observe high rates of unlicensed software use by enterprises, and sales of BSA member software per PC in China remain well below those seen in the global markets and even emerging markets at comparable levels of economic development. In the meantime, although the Chinese government has stated that most government agencies are now using licensed software, BSA continues to urge the Chinese government to adopt effective, transparent and verifiable software asset management procedures, where government agencies conduct audits of the software they have installed to ensure, among other

things, that all copies in use are properly licensed. While there is some hope that on-going intellectual property-related legal and judicial reforms will help address some of these challenges, BSA continues to believe that the primary means of assessing progress is through verifiable increases in the sale of legal software and software related products and services.

BSA urges the US government to continue to closely engage with the Chinese government to make meaningful progress on a range of these issues to ensure fair and equitable market access for BSA members and other US and foreign information and communication technology (ICT) companies. Such engagement should continue via on-going dialogues and negotiations such as the Joint Commission on Commerce and Trade (JCCT), the Strategic and Economic Dialogue (S&ED), the US-China Bilateral Investment Treaty (BIT), and China's accession to the World Trade Organization (WTO) Government Procurement Agreement (GPA), among others.

Market Access

BSA seeks a fair and level field for competition in the software and related ICT market. While ensuring the security of government systems and important economic sectors is rightfully an important priority of the Chinese government, security should not be used as a pretext for adopting measures that act as unnecessary and illegal barriers to market access. Furthermore, market access for software and other ICT products and services should not be limited to those with intellectual property that is locally owned or developed, nor should it depend on the transfer of intellectual property to China domestic firms. Incentives for encouraging investment in research and development (R&D) facilities in China should not include requirement for doing so in order to provide products and services to the market.

Security: In early 2015, the Cyberspace Administration of China (CAC) announced that it had finalized a draft of the National Cybersecurity Review Regime, which is expected to be submitted to the Office of the Central Leading Small Group for Cybersecurity and Informatization for review. Details remain unclear, but the regime may exclude any ICT products or software that are not deemed "secure and controllable" by government authorities. Indications suggest that some of the criteria, such as requirements to disclose source code or turn over encryption algorithms and solutions, are designed to ensure that only domestic products will be eligible to qualify.

The trend is quite alarming. A variety of laws, regulations and policies are under development with very little visibility by, or input from, affected industry stakeholders. BSA urges the US government to engage in an immediate bilateral dialogue to build mutual trust and understanding regarding US and Chinese policies to ensure the security and integrity of ICT networks. Pending such discussions, China should refrain from implementing policies under the guise of cybersecurity that would have the effect of unfairly blocking BSA member products and services from important commercial sectors in China economy.

In addition to the emerging policies, BSA continues to urge amendments to long-standing measures, such as the Multi-Level Protection Scheme (MLPS). The MLPS imposes significant restrictions on procurement of 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 Chinese Government and increasingly to procurements by SOEs and others in the private sector. This results in an undue and discriminatory market access restriction for foreign information security products and will in

many cases prevent information systems in China from procuring the most effective security tools to meet their needs.

BSA welcomed the commitment made by China in the 2012 JCCT that it will review and revise the MLPS rules through a process that will seek the views of all parties, including through dialogue with U.S. parties. BSA urges China to use this process to remove requirements that discriminate against foreign-supplied products and services, or those that have foreign-owned intellectual property.

Procurement: The software industry remains concerned that the Chinese Government is adopting mandates or preferences for domestic software brands for government agencies and SOEs. This is inconsistent both with China's efforts to join the GPA, and with China's commitment in its WTO Working Party Report 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...."

In May 2013, China's Ministry of Finance (MOF) issued new rules on software procurement, the Notice on Generic Software Assets Allocation Standards in Government Agencies (MOF Decree). The MOF Decree imposes price controls and preferred licensing terms (e.g., site-licenses) on procurement of software that favor local brands and significantly restrict market access for foreign brands. Moreover, the MOF Decree focuses on the procurement of only certain types of software – operating systems, office productivity software, and anti-virus software – suggesting that procurement may not be authorized or, at a minimum, that budgets will not be made available for other types of software. This directive does not comport with best practices for software procurement, does not adequately take into account the speed with which software products and services are developing, and puts in place *de facto* preferences for procuring domestic software products and services that are not in keeping with China's JCCT and S&ED commitments to avoid discrimination against products with foreign-owned or foreign-developed intellectual property in its government procurement and its WTO accession obligations to refrain from imposing price controls.

Additionally, China has provided similar guidance to the SOEs. This guidance has been provided directly, as well as on State-owned Assets Supervision and Administration Commission (SASAC) hosted SOE product legalization websites. This guidance: (a) creates a preference to purchase domestic-brand software; (b) erects artificial barriers that impede market access by suggesting that products are comparable when they are not (e.g., business productivity software versus basic word processing software); and (c) presses entities to support, encourage, and ensure the fast growth of the domestic software industry.

BSA urges the Chinese Government to withdraw the MOF Decree and address its discriminatory elements, including by removing the price controls and site-license preference, and refrain from adopting or implementing any other measure that would have the effect of excluding foreign software or favoring domestic software in government procurement. China should also affirmatively declare: (a) that it will not influence, either formally or informally, the software purchasing decisions of SOEs in any way (whether through the MOF Decree or otherwise); and (b) that it will take affirmative steps to clarify to all SOEs that they remain free to make software purchasing decisions based on commercial considerations irrespective of the origin of the software or the nationality of the supplier. In keeping with these commitments, China should remove all instances of such discriminatory guidance from all government websites directed at SOEs.

VATS Licensing: China's authorities, principally the Ministry of Industry and Information Technology (MIIT), require companies wishing to provide Internet-based services or content to acquire VATS licenses. For example, companies wishing to provide web- or cloud-based content services must acquire an Internet content provider (ICP) license. However, foreign invested enterprises are not allowed to acquire such a license. By regulation, foreign firms wishing to acquire such a license must establish a foreign invested telecommunication entity (FITE), which must contain less than 50 percent foreign equity. Worse, in practice, MIIT has not issued new ICP licenses to FITEs.

Similarly, foreign firms are restricted from running data centers in China because they have no opportunity to acquire the necessary Internet data center (IDC) license.

In 2013, MIIT issued for public comment proposed revisions to China's Telecom Services Catalogue. The draft catalogue continues to treat cloud computing and other Internet-based services as VATS which carries significant restrictions on foreign investments. China should use this revision of the catalogue to remove the treatment of such service as VATS.

Encryption: China maintains regulations that state:

- entities importing, developing, and selling encryption technology in China must obtain a license from the State Encryption Management Bureau (SEMB), including a special license to apply to use foreign encryption technology;
- encryption products sold in China must be subject to testing that requires disclosure of source code in order to receive a sales license; and
- foreign technology providers must use Chinese indigenously developed encryption technology, particularly algorithms.

These regulations remain a significant barrier, real and potential, to foreign products, particularly if authorities begin applying the regulations more broadly. These rules runs counter to China's agreement with five other countries in 2013 to adopt the World Semiconductor Council Encryption Best Practices. These Best Practices, among other things, prohibit the regulation of encryption used in commercial ICT products that are imported or sold domestically.

Intellectual Property

Service Invention Regulations: In 2012, SIPO issued draft Service Invention Regulations (SIR) as part of an overall effort to improve incentives for workers to innovate. This is due to the recognition by the Chinese government that many Chinese firms, especially SOEs, are not efficiently commercializing significant R&D investments.

BSA members and many other R&D-intensive enterprises (including many Chinese private enterprises and SOEs) have raised a number of significant concerns regarding these proposed regulations. They are overly prescriptive and could impose obligations with which many companies would find impossible to comply. Even if firms were able to comply, the requirements would be prohibitively expensive. The draft regulations impose obligations to grant ownership rights and compensation for inventions that are not in line with normal business practices. They take a broad view of the term "invention," including trade secrets as well as patented inventions. A major concern to BSA members is a provision that appears

to allow for the invalidation of company policies or employer-employee contracts regarding intellectual property ownership and remuneration if such policies or contracts are deemed inconsistent with the provisions of the draft regulations.

BSA filed comments on each draft of the SIR as it was released for public comment (two in 2012 and most recently in 2014). BSA has also urged the USG to raise this issue in the Joint Commission on Commerce and Trade (JCCT), the Strategic and Economic Dialogue (S&ED) and the Innovation Dialogue. We urge the Chinese government to reconsider the proposed SIR and withdraw them from active consideration pending further study and discussions with affected industry stakeholders.

Intellectual Property and Competition: The State Administration of Industry and Commerce (SAIC), one of three Chinese agencies responsible for Anti-Monopoly Law (AML) enforcement, has been developing "IPR Abuse" or "IPR Misuse" rules over the last two years. BSA members have expressed concern that the drafts take an overly prescriptive view, appearing to designate a variety of normal business practices as anti-competitive and leaving wide discretion to SAIC and its subsidiary agencies to find AML violations for activities not seen as anti-competitive in other jurisdictions. BSA has filed comments with the SAIC on various drafts and has joined other foreign firms and associations in encouraging the USG to raise this issue in bilateral discussions.

Patents and Standards: Multiple agencies have asserted jurisdiction over policy matters related to the treatment of patents in standards development. These include the Standardization Administration of China (SAC), the SAIC and the Supreme Peoples' Court (SPC). SAC has issued three draft "rules" on patents involved in national standards over the last 10 years that would establish rules and procedures for patent holders who own standard essential patents (SEPs). SAIC has also proposed particular provisions related to SEPs in its draft IPR Abuse Guidelines (discussed above). Finally, the SPC has several times proposed JIs that would direct China's courts on how to resolve disputes over SEPs.

BSA has filed comments on all such draft measures, urging that such rules avoid overly prescriptive requirements. It is important that rules governing the treatment of patents in standards strike the right balance between the rights and interests of patent holders and standards implementers. The draft rules often propose to create unreasonable search and disclosure requirements on patent holders, regardless of whether the patents are truly "essential," whether the patent holder is an active participant in the standard setting process, or whether the patent holder has made fair, reasonable and non-discriminatory (FRAND) licensing commitments. The draft measures have also proposed imposing royalty free licensing terms on SEPs, explicitly allow for compulsory licenses, or otherwise restricting the ability of patent holders to freely negotiate FRAND licenses.

The issue of SEPs in China is challenging in light of the evolving nature of China's authorities regarding the use of intellectual property to promote domestic innovation and the explosion of patents in China, including a large proportion of unexamined, low-quality patents primarily granted to domestic Chinese firms. BSA urges the US government to continue active engagement with China in the JCCT and other venues to ensure that such rules do not unfairly discriminate against BSA members.

Patent Enforcement: 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 is improper 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.

Copyright and Enforcement

According to the latest information, the rate of unlicensed software use in China declined from 77 percent in 2011 to 74 percent in 2013. However, this rate remains extremely high, far above the regional (62 percent) and global (43 percent) rates. The estimated commercial value of unlicensed software in China was nearly US$8.8 billion, the largest value by far among all US trading partners.[1]

Government and SOE Licensing/Legalization: Despite numerous specific commitments by the Chinese government to tackle the use of unlicensed software by government agencies and SOEs, BSA remains concerned that software legalization programs are not being implemented in a comprehensive manner. To follow through on its software legalization commitments, the Chinese government needs to implement comprehensive legalization programs for the Chinese government and SOEs that include: (a) audits, certification and other credible processes to verify software license compliance; (b) software asset management best practices; (c) sufficient budgets to purchase legal software; (d) performance indicators to hold government and SOE officials accountable for ensuring measurable progress on software legalization; and (e) a prohibition on mandates or preferences for the purchase of domestic software brands as part of the legalization process.

Statutory and Regulatory Provisions: The third draft of amendments to the Copyright Act now is now under review by the State Council Legislative Affairs Office. There is an urgent need for China to update and modernize its copyright law. BSA urges the Chinese government to quickly enact copyright reform that:

- clarifies that use of unlicensed software by enterprises is a violation of the reproduction right;
- clarifies that unauthorized temporary reproductions, in whole or in part, may be violations of the reproduction right; this will likely become increasingly important to BSA members as business models shift to providing software on the cloud;
- increases statutory damages, at least so that they are in line with the revised Trademark Law;
- ensures that protections for technological protection measures (TPMs) extend to access controls and that the unauthorized sale of passwords and activation codes are explicitly defined as TPM circumvention; and
- strengthens procedural provisions, for example to explicitly grant courts more authority to compel evidence preservation and grant preliminary injunctions.

Unlike Copyright Law reform, reform of China's Criminal Code appears to be moving forward.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

However, BSA's latest information suggests changes to the intellectual property provisions of the Law (e.g., Articles 217 and 218 and accompanying JIs) and other related provisions may not be under consideration. This would be a missed opportunity, and we urge the Chinese government to reconsider this decision. BSA urges that the following issues be addressed and improved:

- Reduce thresholds that are too high (in the case of illegal income) or unclear (e.g., in the case of the copy threshold);
- Provide all commercial scale infringements with a criminal remedy. Because the requirement to show that the infringement is carried out "for the purpose of making profits," is an unclear phrase, law enforcement authorities have been reluctant to hold that commercial enterprises using unlicensed software in the course of their business operations are subject to criminal liability;
- Define, distinct from copyright infringement, criminal violations for circumvention of TPMs and trafficking in circumvention technologies, software, devices, components, and services, including in particular the unauthorized sales of passwords or product activation codes or keys.

In addition to correcting the scope of criminal liability for intellectual property violations, the law should also be amended to lift the jurisdictional bar limiting foreign right holders from commencing a private "civil claim" against those being prosecuted for copyright crimes in local district courts.

Compliance and Enforcement: There are significant hurdles to effectively addressing the use of unlicensed software by enterprises in China. In civil cases, several critical improvements are needed. The courts should relax excessively high burdens for granting evidence preservation orders and need to increase the amount of damages awarded against enterprises found using unlicensed software. While some courts have increased the amount of damages, others, when facing similar infringement situations, grant much smaller "statutory damages" in lieu of a proper compensatory award. This problem highlights the need to increase statutory damages beyond those currently laid out in the third draft of amendments to the Copyright Act. Additionally, in cases in which a civil order is issued, right holders and authorities often face on-site resistance against evidence preservation and have only a limited amount of time to conduct software infringement inspections.

BSA members have observed with interest the establishment of three new specialized intellectual property courts in Beijing, Shanghai, and Guangzhou. These courts operate at the intermediate level, with appeals going to the Beijing, Shanghai, and Guangzhou High Courts respectively. According to the most recently published guidance, these courts have jurisdiction over patent cases and software related copyright cases. Establishing these specialized intellectual property courts is a demonstration by the Chinese government of their increasing interest in building more effective judicial enforcement mechanisms for the protection of intellectual property. BSA is looking forward to observing meaningful improvements in the efficiency and quality of judicial decisions from these courts.

The amended Criminal Transfer Regulations are well intentioned but do not adequately address existing challenges to the effective transfer of administrative cases to criminal investigation and prosecution. The Regulations leave unclear whether transfers are required upon "reasonable suspicion" that the criminal thresholds have been met, and thus, some enforcement authorities believe "reasonable suspicion "is insufficient to result in a transfer, requiring proof of illegal proceeds. Administrative authorities, however, do not employ investigative powers to ascertain such proof. The "reasonable suspicion" rule should be expressly included in amended transfer regulations.

Recommendation: Due to continuing high levels of unlicensed software use by enterprises and a deteriorating market access environment for the ICT sector, BSA recommends that China be maintained on the Priority Watch List.

INDIA

Although there are positive signals regarding both market access for information and communication technology (ICT) products and software, as well as the enforcement of intellectual property, BSA recommends that India be maintained on the Priority Watch List because of the challenges faced by BSA members in providing products and services to the market and the persistently high rates of unlicensed software use by enterprises.

Overview/Business Environment

A series of government announcements by the new administration such as the establishment of the Digital India initiative, the activation of the Copyright Enforcement Advisory Council, and the constitution of the new Think Tank on Intellectual Property Rights (IPR) by the Department of Industrial Policy and Promotion (DIPP) are all positive developments. These initiatives, however, are only beginning, and because the recommendations of the committees have yet to be implemented, it is premature to assign actual improvements to the commercial environment based on these developments. In addition, it is disappointing that some of the key committees, such as the Copyright Enforcement Advisory Board, have not included multinational companies or their representatives in their deliberations.

As a practical matter, the commercial environment for BSA members remains challenging in India. In addition, in some policy and regulatory matters, such as those related to cross-border data flows and requirements to localize data and servers in country, there are some signs that the environment could deteriorate rather than improve. Government procurement policies remain outmoded and inefficient because of local content preferences. Many such policies do not offer a level playing field to foreign technology providers who are keen to bring cutting edge technologies and services to India.

The unlicensed use of software by enterprises in India remains high as well. The most recent information indicates that the rate of unlicensed use of software in India is 60 percent, representing a commercial value of unlicensed software of US$2.9 billion.[1] This alarming figure highlights the scope of the problem and underscores the importance of making more progress against the use of unlicensed software by enterprises in India.

While the legal and judicial systems are effective in bringing enforcement actions against such enterprises, damage awards tend to be low, and consequently such cases fail to deter further unlicensed use of software. On a more positive note, a number of government agencies and enterprises have been receptive to the fact that the use of licensed software reduces unnecessary risks to their information and communication technology (ICT) systems and BSA hopes that this awareness can be spread more widely throughout India's ICT ecosystem.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Market Access

The Indian government, at the central and state levels, has adopted a variety of policies affecting the commercial environment for BSA members and the ICT sector more generally. Such policies have been developed and adopted without adequate consultation with stakeholders. In addition, they are often implemented in confusing and inconsistent manners. This has created a substantial and negative impact on ICT sector investment and growth in India. Domestic preferences in public procurement and a confusing regulatory environment regarding security and privacy have dampened the enthusiasm of many BSA members for the Indian market. BSA and our members are eager to work with the new administration to foster a more transparent and effective policy environment that will drive investment and deployment of cutting edge technologies and service solutions, which will in turn drive the digital economy and benefit Indian businesses, government agencies, and consumers alike.

Cross-Border Data Flows: BSA urges India to remove data- and server-localization requirements that have been imposed in a heterogeneous manner across regulatory structures and procurement contracts throughout 2014. There is strong evidence that such policies are harmful to India as they reduce productivity and dampen domestic investment in the country.[2]

Encryption: India lacks a uniform and effective encryption policy. Most other countries allow the usage of strong encryption standards ranging from 128-bit to 256-bit to ensure the security of sensitive information exchanged via the Internet and other networks. In India, however, only 40-bit encryption can be used without additional regulatory approval according to the Department of Telecommunications' Guidelines for the Grant of License for Operating Internet Service (ISP Guidelines). Encryption standards differ greatly from one regulatory agency to another, each having their own specific standards.

Privacy: Ensuring the confidence of customers that their sensitive data will be protected and maintained appropriately is a major concern of most online service providers, including BSA members who increasingly offer data services to their customers. A draft privacy bill, which is intended to address issues pertaining to privacy compliance and provide confidence to companies looking to do business in India has yet to be passed by Parliament. Further, the bill creates several broad exceptions that are susceptible to misuse or misinterpretation, including by law enforcement agencies. BSA looks forward to further opportunities to improve the draft privacy legislation.

Intellectual Property

National IP Policy: India announced the development of the National Intellectual Property Policy through the constitution of an IPR Think Tank comprised of eminent judges, legal luminaries, and other eminent citizens. On December 19, 2014 the first draft of the National IPR Policy was submitted by the IPR Think Tank. The draft intends to strengthen the existing laws on intellectual property and provide equally strong administrative and procedural mechanisms, as well as improved judicial infrastructure. The draft policy, however, does not consider amendments to provide for statutory damages or allow for summary trials in intellectual property-related matters.

[2] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

The draft policy states that following steps will be taken, *inter alia*, to achieve its objectives:

- Establishing a centralized Multi-Agency Task Force for coordination between the various agencies and providing direction and guidance on strengthening enforcement measures; and
- Recommending a specialized patent bench in the High Courts of Bombay, Calcutta, Delhi, and Madras for speedy disposal of patent cases.

BSA filed written comments to the IPR Think Tank on the draft National IP Policy on January 30, 2014. Our comments, *inter alia*, recommended:

- establishing a National IP Enforcement Taskforce;
- enacting an effective trade secret protection law;
- modernizing the current Copyright Law including the adoption of statutory damages and a clarification that temporary reproduction may be subject to copyright;
- ensuring the patentability of eligible computer-related inventions; and
- adopting procedural reforms to reduce the patent backlog, and a cautious approach when considering the adoption of a utility model patent system.

Compliance and Enforcement: The lack of statutory damages and significant damage awards in civil enforcement continues to be a challenge for BSA and our members. Indian courts have been reasonably prompt in granting preliminary or interim injunctions, but the system suffers from significant procedural delays.

The software sector has maintained good engagement and positive relationships with enforcement authorities. Criminal enforcement, however, is not a practical approach for enforcing against enterprise use of unlicensed software. This is primarily because of the rigidity of the criminal judicial system and the increased pressure on the enforcement authorities to address the major crimes and serious offenses, making an effective civil enforcement system all the more important. Criminal enforcement of software related crimes, therefore, tends to focus on channel piracy (e.g., hardened criminals reproducing and distributing pirated or counterfeit copies), as opposed to enterprise use of unlicensed software.

Technical Assistance and Education: BSA is actively engaged with the government of India on a variety of matters. BSA and our members have worked closely with various Indian, American and global industry associations and trade bodies to raise a variety of issues. The following are examples of BSA engagement with various government agencies, including at the state and local level.

- BSA, in partnership with the Federation of Indian Chambers of Commerce and Industry (FICCI), developed an IPR Tool Kit for Customs, which was released on December 11, 2014. Captain Sanjay Gahlot, Commissioner, Commissionerate of Customs, Ahmedabad and 18 customs officials participated in a capacity building program that was held at the time of the toolkit release. The development and launch of the IPR Tool Kit for Customs officials is part of a series of initiatives pursuant to the Memorandum of Understanding (MoU) signed between FICCI and BSA, where the two organizations agree to work together to create awareness regarding the harm of intellectual property infringement and capacity building for enforcement agencies on intellectual property enforcement.

- BSA is a member of the government's Copyright Enforcement Advisory Council (CEAC) Sub-Committee led FICCI. In this role, BSA actively supported (a) drafting the Standard Operating Procedures for Police on Copyright Enforcement and (b) developing a chapter on "Issues Faced by the Industry Regarding Enforcement of Copyrights and by Police Officials while Dealing with IPR Matters." The final report was submitted by FICCI to CEAC in August 2014.

- BSA and FICCI, in partnership with the State Government of Gujarat, launched an advertisement campaign from August 19-22, 2014 promoting use of original software and highlighting the risks of using unlicensed software in various local newspapers in Gujarat.

Recommendation: Although there are positive signals regarding both the market access situation for ICT products and software, as well as the enforcement of intellectual property, BSA recommends that India be maintained on the **Priority Watch List** because of the challenges faced by BSA members in providing products and services to the market and the persistently high rates of unlicensed software use by enterprises.

INDONESIA

Due to a worsening market access environment for the information and communication technology (ICT) sector, rampant levels of unlicensed software use, and continuing deficiencies in legal enforcement mechanisms, BSA recommends that Indonesia remain on the Priority Watch List.

Overview/Business Environment

The commercial environment for the information and communication technology (ICT) sector in Indonesia is very challenging. A variety of authorities have issued, or are in the process of developing, policies that will raise the cost of providing digital products or services to the Indonesian market. In addition, the use of unlicensed software by enterprises in Indonesia is among the highest in the region, affecting the legitimate market and putting such enterprises at risk for security vulnerabilities and malware.

The recently enactment of the new Copyright Law No. 28/2014 was a positive development last year, but the new law must be implemented effectively. Intellectual property enforcement remains extremely difficult. Enforcement authorities are under-resourced and criminal actions are rare. Civil litigation is an option, but because damage awards tend to be so low, such actions are quite costly to the plaintiffs and do not send a deterrent signal to the market.

Market Access

A variety of policies affecting the ICT industry have been developed or proposed over the last several years that make, or threaten to make, it increasingly difficult to provide digital products and services to the Indonesian market.

Data Localization Requirements: The Ministry of Communications and Information Technology (MCIT) is in the process of developing implementing rules for Government Regulation No. 82 of 2012 on the Implementation of Electronic Transactions and Systems (GR 82). There is considerable uncertainty regarding certain key concepts and the scope and implementation of the regulations. Depending on these specifics of the implementing regulations, GR82 could require data service providers, including cloud service providers, to locate data centers in Indonesia as a condition of providing online services. Such data localization rules undermine the benefits that a globally distributed infrastructure can provide to consumers, enterprises and small businesses around the world. BSA urges MCIT to reconsider the regulations and avoid imposing such data and server localization requirements.

Local Content Requirements: A more recent MCIT proposal, the Ministerial Decree on Local Content for LTE Technology, would impose onerous local content requirements on a wide range of technology devices and products. The decree is expected to be signed by the end of March and strictly enforced by the beginning of January 2017. The rules envision all products imported into Indonesia would need to consist of 20-40 percent local content, although the meaning of "local content" remains to be defined. The purpose of the measure is to encourage local industry development. The regulation, however, will effectively block foreign companies without local production facilities from the Indonesian market, and require companies who wish to support the market to restructure their global supply chains. This in turn will reduce the supply and therefore raise the costs to consumers and enterprises in Indonesia who wish to

purchase and use such products, as well as increase the grey market for products that are excluded from the market. We believe that Indonesia can better achieve its objective to develop the local ICT industry by creating incentives that will attract production facilities to Indonesia on the merits of the local commercial and regulatory environment rather than by penalizing companies with global supply chains that strive for greater efficiency and economies of scale. There is also an opportunity for Indonesia to enhance higher value-added sectors such as in software and application development that are more sustainable in the longer term than focusing on low-cost manufacturing.

Copyright and Enforcement

According to the latest data, 84 percent of the software used in Indonesia is not licensed. This is one the highest rates in the region and represents a commercial value of US$1.46 billion in unlicensed software.[1]

Statutory and Regulatory Provisions: Indonesia enacted a new copyright law in 2014. The new law clarifies that software is copyrightable and provides protection for "compilations of creations or data in a format that can be read by computer programs or other forms of media." Because the law provides circumstances in which temporary reproductions are not considered infringement, it appears to implicitly accept that some temporary reproductions do infringe. Importantly, the law now provides prohibitions against the circumvention of technological protection measures TPMs, including both access controls and copy controls, but clear provisions prohibiting trafficking in devices, technologies, and services primarily designed to circumvent TPMs are still needed.

Compliance and Enforcement: There was little improvement in enforcement in 2014. Police will support conducting raids against companies using unlicensed software, but as a general matter criminal enforcement actions for software copyright infringements are rare and prosecutors rarely receive cases from police or the Intellectual Property Office's enforcement officers (PPNS).

Few civil copyright infringement cases are initiated. This is partly because of very low damage awards given by judges. Legal expenses are not recoverable so the plaintiff has to bear the costs of bringing proceedings. On the other hand, cases brought before the Commercial Court are processed relatively quickly, taking around three months to conclude.

The courts in Indonesia remain largely ineffective for civil and criminal enforcement against software copyright infringement and enterprise use of unlicensed software. To improve matters, it is first critical to improve the quality and consistency of civil Commercial Court rulings. The Commercial Court should, like the Supreme Court, publish its decisions and provide official copies to the parties as a matter of course to improve transparency and reduce irregularities. Second, Commercial Court judges should receive training to improve their understanding of how intellectual property cases are conducted. The training should address such matters as damages calculations; issuing provisional orders; and implementing injunctions, and should be expanded to Commercial Courts of Indonesia beyond Jakarta, especially in Medan, Semarang, Surabaya, and Makassar.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Technical Assistance and Education: BSA was involved in several programs in 2014, including: a US Chamber of Commerce and AmCham Indonesia workshop on Digital Trade and Cross-Border Data Flows, a European Union intellectual property technical cooperation program, and a British Government technical program on intellectual property.

Recommendation: Due to a worsening market access environment for the ICT sector, rampant levels of unlicensed software use, and continuing deficiencies in legal enforcement mechanisms, BSA recommends that Indonesia remain on the **Priority Watch List**.

RUSSIA

Due to recently enacted onerous market access restrictions and persistently high levels of unlicensed software use, a lack of political will to prioritize intellectual property enforcement, and on-going challenges in the administrative and judicial systems, BSA recommends that Russia remain on the Priority Watch List.

Overview/Business Environment

The commercial environment for BSA members is bleak. Onerous regulatory requirements and discriminatory procurement policies threaten the ability of foreign software, Internet and other information and communication technology (ICT) firms to provide products and services to the market. In order to ensure that Russian business, consumers, and government agencies continue to have access to the cutting-edge technologies that BSA members can provide, these proposed or enacted policies need careful review and reconsideration. The US government should engage in consultations with the Russian government to convince them to meet their international trade commitments and refrain from imposing unjustified restraints on trade and investment.

Russia's intellectual property enforcement remains deficient. It is essential that the government of Russia, as it did prior to accession to the World Trade Organization (WTO), again recognize the importance of tackling copyright infringements. Law enforcement authorities must pursue more criminal and administrative actions against enterprises using unlicensed software, strengthen administrative penalties, particularly against large-scale enterprises, and seek deterrent administrative and criminal penalties from the judicial authorities.

Market Access

Cross-Border Data-Flows and Server Localization: Federal law N 242-FZ, which will come into force on September 1, 2015, obliges all relevant entities, including Russian entities, to store personal data collected from Russian citizens in servers located in the territory of the Russian Federation. Any firm collecting or processing such data is obliged to inform Roscomnadzor of the location of the database prior to collection. In case of non-compliance, the federal law empowers Roscomnadzor to block access to unlawfully collected personal data and establishes detailed procedures for the blocking web sites and other Internet services storing or processing such personal data. While some of the requirements of this law remain unclear and require additional guidance from the government, it appears to be one of the most restrictive data localization laws in the world. As such, it will severely hamper the ICT industry in Russia for both foreign and domestic providers.

Procurement: BSA is concerned about potential measures to amend government procurement policies to favor the acquisition of domestically developed ICT products, including software. Many of these proposals are under discussion. For example, the criteria for domestically developed ICT products, the margin of preferences afforded to domestic providers and contract price mandates are all under consideration. BSA recommends that the Russian government consider other means of promoting its domestic ICT sector in ways that will not deprive government agencies of the cutting-edge technologies and services they need to meet their missions.

Other Market Access Issues: The State Duma is considering legislation that would prohibit foreign legal entities from rendering cloud services to state and local authorities. If enacted, this policy will deprive the Russian economy from benefiting from the best technologies and technology services available.

Copyright and Enforcement

Enterprise Licensing/Legalization: According to the latest BSA information, the use of unlicensed software in Russia continues to drop, but it still at 62 percent. This represents a commercial value of = over US$2.6 billion in unlicensed software.[1]

Government and SOE Licensing/Legalization: Government software legalization decreases risks to the security of the systems and helps change public perception of the need to license software properly. To set the right example for the market for legitimate sale of software products and services, the Russian government should use legal software and develop procedures for the acquisition of licensed software from Russian and foreign software vendors by government institutions and state owned enterprises. The adoption of effective, transparent, and verifiable software asset management procedures, where government agencies conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed, could also provide a powerful positive example to private enterprises.

Compliance and Enforcement: For the past several years, the number of actions by police has declined significantly. 2014 witnessed an acceleration of this troubling trend. This has been due, in large part, to a reduction in the number of police assigned and adequately trained to investigate intellectual property crimes. Fundamentally, the decline in enforcement activity is attributable to a complete lack of political will to address intellectual property crimes and consequently intellectual property enforcement has been deprioritized. New and inexperienced police officers are now frequently in charge of intellectual property issues, and they are hesitant to work on intellectual property cases because intellectual property crimes are viewed as a low priority by their supervisors. Enforcement efforts are further undermined by a reluctance on the part of law enforcement to pursue actions against large scale infringers. Unsurprisingly, in 2014 BSA observed a decline in virtually every statistical category related to enforcement, including the number of criminal actions and investigations taken against targets suspected of using unlicensed software, the number of criminal cases brought to trial, and the number of administrative enforcement actions conducted.

Currently, administrative penalties imposed on enterprises using unlicensed software are far too low to serve as a deterrent against further infringements. Because it is not uncommon for administrative fines to be less than the cost of obtaining a legitimate license, the law creates a perverse incentive for enterprises to use unlicensed software.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

In the rare instance that an investigation results in the filing of a civil or criminal complaint, BSA continues to experience a number of obstacles in Russian courts. Russian judicial practices and procedures should be clarified to establish guidelines regarding: (a) the quantum of evidence necessary to establish a defendant's criminal intent; (b) the methodology for determining the value of infringing copies; (c) the evidence necessary to obtain provisional measures; (d) the implementation of provisional measures; and (e) the use of post-raid materials as evidence.

In a number of regions of Russia, courts do not inform right holders of court hearings on infringement-related administrative cases and pass decisions in the absence of rights holders' representatives. Such an approach leads to violations of procedural rights and the legitimate interests of software producers. BSA members do not always receive up-to-date and necessary information about administrative cases, which may cause their legal representatives to be absent from the proceedings.

Recommendation: Due to persistently high levels of unlicensed software use, a lack of political will to prioritize intellectual property enforcement, on-going challenges in the administrative and judicial systems, and onerous market access barriers, BSA recommends that Russia remain on the **Priority Watch List**.

VIETNAM

Due to extremely high levels of unlicensed software use by enterprises and government institutions, as well as a number of increasingly troubling information technology (IT) regulatory measures, BSA recommends that Vietnam be listed on the Priority Watch List.

Overview/Business Environment

2014 saw a new wave of institutional reform, some with potentially positive effects in the overall investment environment. Unfortunately, many measures for regulating the information technology (IT) sector will reduce fair and equitable market access for BSA members wishing to provide software products and online services in Vietnam. In 2014, Vietnam adopted market access restrictions on server location and procurement that threaten the ability of foreign IT service companies to compete in the marketplace. Also, unlicensed software use remains very high, both in the private and public sectors. BSA received positive support from Ministry of Culture, Sports and Tourism (MCST) and the High Tech Crimes Department of the Public Security Ministry (High Tech Police) in addressing the unauthorized use of software by enterprises in Vietnam.

Market Access

Vietnam has enacted, implemented, or proposed a number of draft laws or regulations that will likely impose restrictions on the cross-border transfer of data or require local server localization in Vietnam These measures will not only hamper the ability of BSA members and others in the IT sector to provide innovative products and services to the Vietnamese market, they may also conflict with commitments to ensure the freedom to transfer information being negotiated in the Trans-Pacific Partnership (TPP) agreement.

Cross-Border Data-Flows and Server Localization: On September 1, 2013, Decree No. 72 went into force.[1] The decree, and other measures reportedly being considered on IT services, appears to impose onerous requirements on server localization and restrictions to cross-border data flows that will undermine the ability of BSA members to provide digital services in Vietnam. Specifically, Article 4.2.e of the Decree No. 72 implementing guidance, requires that website operators and social network service providers must have at least one server system in Vietnam to allow for inspection, storage, and provision of information at the request of competent authorities.[2] This may impact the ability of BSA members to provide software-based services on-line (e.g., cloud computing), which offers many potential economic benefits, especially to small- and medium-sized enterprises in Vietnam.

More recently, BSA and our members have raised renewed concerns regarding the revised IT Services Decree regulating the provision of IT services in Vietnam. BSA filed comments in 2012 on an earlier version of this measure. A revised draft was issued last year by the Ministry of Information and Communication (MIC) for public comment. While some of our comments from that submission appear to have been taken into consideration, we remain concerned about a number of elements of the proposed

[1] Decree No. 72 72/2013/NĐ-CP on the Management, Provision, and Use of Internet Services and Online Information

[2] Ministry of Information and Communication's Circular No.09/2014/TT-BTTTT

decree that would seriously impact BSA members' ability to provide products and services to the market and may be inconsistent with Vietnam's domestic economic development objectives and its international commitments. Specifically, the draft decree appears to restrict cross-border data flows, impose unnecessary requirements to localize hardware (e.g., servers) in Vietnam, and require unwieldy certification requirements for IT service professionals, among other things. For these reasons and others, BSA urges the government of Vietnam not to issue this decree.

Over-The-Top Services: MIC issued a draft circular on November 6, 2014 (ver. October 28, 2014) concerning the management, provision and use of Internet-based texting and calling services (commonly referred to as "over-the-top" or "OTT" services). The draft circular contains onerous obligations that would significantly and negatively affect the ability of BSA members to provide OTT services in Vietnam. These include server localization requirements, a requirement for fee-based OTT service providers to enter into commercial agreements with domestic Vietnam telecommunications companies, and onerous and overly-broad reporting obligations. It will be necessary for the Vietnam government to engage in further stakeholder dialogue to explore alternative, non-trade-restrictive ways of addressing the underlying concerns behind the draft circular.

Procurement Discrimination: MIC issued a circular, dated February 20, 2014, establishing a preference to purchase Vietnam-made IT products and services by government agencies and other entities funded by the state budget.[3] Vietnam-made IT products or services are defined as those products produced or services provided in Vietnam by entities, the dominating shareholders of which are Vietnamese. Government procuring entities must provide full justifications for not purchasing Vietnam-made IT products or services.

Another MIC issued circular, which went into effect on January 20, 2015, specifies preferences for open source software in government software purchases.[4] BSA wishes to reiterate its view that open source solutions can and should be part of IT solutions, but purchasing decisions should be made based on the IT needs and the total life-cycle cost of competing solutions, rather than on *a priori* mandates preferring certain licensing models or product lines over others.

Copyright and Enforcement

The rate of unlicensed software use is extremely high in Vietnam, far exceeding the global (43 percent) and regional (62 percent) averages. The latest data indicates that the rate remained at 81 percent in 2013, representing a commercial value of unlicensed software of US$620 million.[5]

Enterprise Licensing/Legalization: Enterprises in Vietnam, including foreign-invested enterprises, tend to place a very low priority on purchasing and using licensed software. BSA enjoys positive support from the Ministry of Culture, Science and Tourism (MCST) and the High Tech Crimes Department of the

[3] Ministry of Information and Communication's Circular No.1/2014/TT-BTTTT

[4] Ministry of Information and Communication's Circular No. 20/2014/TT-BTTTT

[5] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Public Security Ministry (High Tech Police) in addressing unauthorized use of software by enterprises in Vietnam, with administrative actions against such actors increasing from 14 in 2012 to 34 in 2014.

Government and SOE Licensing/Legalization: BSA engaged in discussions with MIC in 2014 on establishing legalization procedures for public entities and the need for the government to avoid mandates or preferences for certain types of software as part of its legalization program. Unfortunately, these efforts have failed to materialize in any concrete initiatives, and MIC did not show interest in taking further steps after first round of discussion. In a recent encouraging development, however, MIC's Vice Minister, Dr. Nguyen Minh Hong has signaled interest in having BSA and MIC restart their dialogue on Vietnam government software legalization to ensure effective and legal usage of software within government agencies.

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code (as last amended 2009), the Criminal Code (as amended in 2009), and the Administrative Violations Decree which took effect December 15, 2013.[6] The Civil Code operates in parallel.

Although criminal enforcement has proven to be an ineffective method for addressing the use of unlicensed software by enterprises, the Criminal Code, as amended, criminalizes "commercial scale" acts of "[c]opying of works, audio recordings and visual recordings" or "[d]istributing the copies of work, audio or video recording." While amended Article 170a improved Vietnam's statutory framework in some respects, it is now weaker than the provision in force up until its adoption, the February 2008 Criminal Circular.[7] [8] The Vietnamese government should immediately issue implementing guidance for the Criminal Code to confirm that all infringement can be subject criminal liability, and to confirm that "commercial scale" infringements are not limited to those undertaken with a profit motive.

The Administrative Violations Decree, which took effect December 15, 2013, seems to be an attempt to fine-tune administrative enforcement mechanisms.[9] Instead, it may send the wrong signal as it reduces the maximum administrative fines available for organizations infringing copyright.

Amendments to the Intellectual Property Code have made a number of improvements in the overall protection of copyright in Vietnam. BSA recommends introducing pre-established damages upon the election of the right holder, which can be very important in civil cases when the harm of the infringement is difficult to calculate.

[6]Decree No. 131/2013/ND-CP on Sanctioning Administrative Violations of Copyright and Related Rights, entry into force December 15, 2013 (replacing Ordinances No. 47 and 109).

[7]For example: 1) the phrase "and for commercial purposes" was removed from the Criminal Code, so the standard for criminal liability is now "on a commercial scale" and technically aligned with the TRIPS minimum standard; and 2) fines are increased to a range from US$2,350 minimum to US$23,500 maximum, and for crimes committed in "an organized manner" or for recidivism, fines are increased to a range from US$18,800 minimum to US$47,000 maximum.

[8]The 2008 Circular criminalized all acts of "infringement" by referring to Articles 28 and 35 of the Intellectual Property Code, including all acts of infringement defined therein, as well as violations involving circumvention of TPMs, decryption of encrypted satellite signals, and other acts.

[9] Decree No. 131/2013/ND-CP on Sanctioning Administrative Violations of Copyright and Related Rights, entry into force December 15, 2013 (replacing Ordinances No. 47 and 109).

Compliance and Enforcement: BSA relies on administrative enforcement, although fines remain too low to constitute an effective deterrent. BSA is working in partnership with the Vietnam Copyright Office and Inspectorate of MCST in the fight against unlicensed software in Vietnam (Partnership in Protection of Software Copyright was established in 2008). 34 administrative enforcement actions were initiated. Fines issued remain very low, in the range of VND20-50 million (roughly US$1,000 – US$2,000), which is less than 10 percent the maximum applicable fine. This reluctance to impose deterrent penalties hampers the ability to make real progress against the unlicensed use of software by enterprises in Vietnam.

The general inactivity of the courts in dealing with copyright infringement issues remains a problem in Vietnam. To BSA's knowledge, no criminal copyright infringement case has ever been brought to the courts in Vietnam due to the lack of implementation guidelines for the revised Penal Code, which went into effect on January 1, 2010. Building intellectual property expertise must be a part of the overall judicial reform effort.

Also, there have been relatively few civil court actions involving copyright infringement in Vietnam to date. Complicated procedures, delays, and a lack of predictability in the outcome contribute to this problem. That said, BSA brought one case to civil court in 2014 and hopes that over time, civil remedies will be available to supplement administrative, and eventually, criminal enforcement.

Technical Assistance and Education: BSA is working in partnership with the government's Inter Ministerial IPR Protection Task Force (Program 168), consisting of representatives of all intellectual property related ministries, including Police, Supreme Court, Supreme Procuracy, Customs, Market Management Force, Ministry of Justice, Ministry of Science & Technology. Our first joint effort will be a 2015 Intellectual Property Day campaign, where both educational and enforcement campaigns will be conducted during the period of March 27 – April 30, 2015.

At the request of Vietnamese enforcement authorities, BSA provided a retraining seminar for 3 MCST's inspectors, 10 officers from High Tech Crimes Department and 10 attorneys on October 24, 2014 in Ho Chi Minh City in order for BSA's members to provide updates on their products and licensing policies. This program was designed to improve the authorities' ability to recognize and record unlicensed software during administrative actions.

Recommendation: Due to extremely high levels of unlicensed software use by enterprises and government institutions, as well as a number of increasingly troubling IT regulatory measures, BSA recommends that Vietnam be listed on the **Priority Watch List**.

Watch List

BRAZIL

Due to an increasingly challenging market access environment for BSA members and continued challenges with high levels of unlicensed software use by enterprises, BSA recommends that Brazil be maintained on the Watch List.

Overview/Business Environment

The overall market environment in Brazil is challenging. A variety of existing and proposed measures related to cybersecurity, privacy, and domestic procurement preferences have created, or threaten to create, *de facto* market access barriers to BSA members' products and services. On the other hand, the environment for intellectual property protection and enforcement has generally improved in Brazil, with BSA and its members enjoying cooperation with law enforcement and working within a generally satisfactory judicial system. More remains to be done, however, to improve the efficiency and reduce the costs of intellectual property enforcement, and to bring down the high rates of unlicensed software use in the country.

Market Access

The market access environment in Brazil for BSA members and the global information and communication technology (ICT) sector more generally has become increasingly challenging. A variety of policies, ranging from Internet governance and privacy, to local content requirements and domestic preferences in government procurement present barriers affecting the ability of BSA members to compete effectively in the market and provide the cutting edge technologies and services increasingly demanded by Brazil's growing businesses. Concerns about privacy and security have been used to justify a variety of barriers to foreign software and ICT products with the result that Brazil's government agencies and enterprises may be left with less mature alternatives. This situation may, paradoxically, increase risks of security vulnerabilities and decrease the confidence of Brazilian consumers that their sensitive personal data will be appropriately protected.

Privacy Legislation: Brazil's long-debated Draft Bill Protecting Personal Data addresses the perceived need for legislation governing the personal data of Brazilian citizens. Since industry and civil society successfully urged Congress to drop onerous provisions for data center localization from the final text of the Marco Civil da Internet Law (Marco Civil), focus has shifted to the Draft Bill Protecting Personal Data to address outstanding aspects of personal data protection and privacy. A draft bill was released for public comment on January 28, 2015.

BSA is analyzing this most recent draft and looks forward to providing comments to the government of Brazil in the coming weeks. BSA urges Brazil to ensure that the framework for protecting personal information that it ultimately adopts will facilitate, rather than impede, the cross-border data transfers that are critical to growth and innovation in the global digital economy.

This most recent draft establishes that data belongs to the individual and cannot be sold to third parties without explicit consent of the individual. From a technical perspective, the bill prohibits linking databases of personally identifiable information if not directly related to furnishing the intended service or

in the absence of consent from the individual. The bill envisions specific timeframes for data retention at the expiration of which controllers must obtain consent. Additionally, the bill only permits personal data to be transmitted to countries with equivalent protections unless the subject consents. Notably, there are many vague terms in the draft bill that will need further clarification in order to assess their potential impact on BSA members operating in the market.

Government Procurement Restrictions: Presidential Decree 8135/2013 (Decree 8135) regulates the use of ICT services provided to the federal government by private and state owned companies. The Ministries of Planning and Defense issued the first set of implementing regulations on May 5, 2014. The Decree states that federal entities and mixed capital ownership companies are restricted to approved state-owned suppliers (e.g., Telebras, Serpro, and Dataprev) that they can contract without bids. Full migration to approved systems must occur within five years.

The Ministry of Planning is currently developing regulations to enable implementation of Decree 8135 which include: technical specifications for standardized services; contract rules, conditions and prices; interoperability standards (referred to as e-PING); management of agency solicitation of services; and periodic price review. The draft regulations present multiple serious problems for BSA members, especially deviation from global standards and requirements to disclose or register source code and other intellectual property. BSA appreciates the opportunity provided by the Ministry of Planning to contribute input via public written comments, which we submitted in late 2014, and through subsequent meetings to be held in late February 2015. BSA hopes that, as a result of this dialogue, the Brazilian government will implement measures that effectively enhance the cybersecurity of government agencies without imposing unnecessary market access barriers to BSA member products and services.

Government Procurement Preferences: CERTICs (Certification of National Technology Software and Related Services) is the certification component of the *TI Maior* Industrial Plan conferring public procurement preferences to software developed in Brazil. Annex I of Decree 8186/14 (January 17, 2014) establishes an 18 percent price preference for the following categories: software licenses; software application development services (customized and un-customized); and maintenance contracts for apps and programs. To date, nine Brazilian companies (TOTVS being the largest) have certified 10 software packages. No non-Brazilian companies have yet been certified.

In addition, proposed legislation (PL 2269/1999) would require the obligatory use of open source software by government entities and state-owned enterprises (SOEs). The legislation had been stalled for some time, but BSA has learned that the bill may have recently gained some legislative momentum. BSA has consistently argued that procurement decisions should be based on choosing the best products and services available to meet the specific requirements without preferences or mandates based on particular technologies or licensing models, taking into account the entire life-cycle cost of a product or service and not just the upfront fees or royalties.

Copyright and Enforcement

According to the most recent data, the rate of unlicensed software use in Brazil is 50 percent. This represents a commercial value of US$2.8 billion in unlicensed software.[1] This is a far greater value of unlicensed commercial software than that measured in any other country in the region.

Compliance and Enforcement: BSA concentrates most of its efforts on bringing civil judicial actions against enterprises that are using unlicensed or under-licensed software. BSA's enforcement campaign is based on an out-of-court cease-and-desist letter procedure aimed at legalizing the use of business software. BSA escalates to filing civil lawsuits against specific companies when it becomes clear that they will not agree to comply with software licenses.

BSA's relationship with the enforcement authorities in the past year improved due to increasing awareness of intellectual property-related issues. While civil cases continue to encounter court backlogs, judges in several major jurisdictions are responding well to requests for trials. Additionally, *ex parte* measures are available when necessary, and the courts order the companies to cease using unlicensed software.

The Superior Court of Justice has reaffirmed earlier rulings that it is not sufficient simply to order companies to pay the license fee they would have had to pay in the first place for the software they have been using without authorization. Instead, fines of multiple times the market value of the unlicensed software are increasingly being imposed. This provides greater deterrence in those cases that proceed to final judgment, but also sends a message to companies that they should not wait to be sued before legalizing their software use.

While these are positive trends, there is room for improvement. Brazilian courts continue to require extremely high fees for forensic experts who conduct searches and seizures and analyze the results. Further, the requirement that companies headquartered abroad must pay bonds to guarantee eventual damages during the civil procedures has proven unreasonable at times. BSA has paid bonds as high as US$25,000.

The National Council to Combat Piracy and Intellectual Property Crimes (CNCP), under the Ministry of Justice, is the main governmental entity responsible for the central coordination and implementation of Brazil's national anti-piracy campaign. After the recent resignation of Flávio Crocce Caetano from his position as CNCP president, it remains critical for the Ministry of Justice to ensure that the reorganized CNCP continues to work closely with industry, that it is adequately resourced, and that it vigorously follows up on its initial steps to expand its work beyond its traditional focus on counterfeiting and piracy of physical goods.

Government Engagement: BSA signed a cooperation agreement with the government of Santa Catarina, which has agreed to support BSA's awareness raising efforts in that state. The government of

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Santa Catarina has already supported training of civil court experts in the city of Joinville, the University of Joinville and the local branch of the Brazilian Bar Association.

Recommendation: Due to an increasingly challenging market access environment for BSA members and continued challenges with high levels of unlicensed software use by enterprises, BSA recommends that Brazil be maintained on the **Watch List**.

BULGARIA

Due to continuing high levels of unlicensed software use by enterprises, especially small- and medium-sized business, as well as concerns about the commitment of prosecutors to pursue much needed criminal enforcement actions, BSA recommends that USTR maintain Bulgaria on the Watch List.

Overview/Business Environment

The business environment for BSA's members remained challenging in 2014 despite Bulgaria's advanced Internet infrastructure and ambitions to serve as an incubator for high tech industries.

In 2014, Bulgaria did not make meaningful improvement in its intellectual property legislation and enforcement regime. In particular, there has been no progress on the development of a new penal code. Enforcement difficulties persisted and, in some cases, worsened.

Copyright

According to the latest data, the rate of unlicensed software use in Bulgaria is 63 percent. That represents a commercial value of US$101 million in unlicensed software.[1]

In 2014, no government-led intellectual property awareness campaigns were planned or executed. The Ministry of Culture's Copyright and Neighboring Rights Inspectorate also suffered from setbacks, resulting in continued reductions in staff to just three inspectors for all copyright claims. Overall, the volume of intellectual property enforcement actions remained insufficient.

Statutory and Regulatory Provisions: Discussions over a new penal code have been sporadic since 2012. Although BSA was invited to participate in public consultations on a possible new draft in early 2014, no tangible results have been produced and there is concern that private sector stakeholders have been excluded from subsequent work on the draft penal code. BSA urges the government of Bulgaria to ensure that the development of the penal code is conducted in an open and transparent manner, with the opportunity for private intellectual property stakeholders to participate in deliberations on this important matter.

Compliance and Enforcement: In 2014, BSA provided leads and assisted local authorities in conducting a total of 14 enforcement actions. BSA also launched the first wave of a direct mailing campaign in which 100 local legal entities were informed about the technical and legal risks of using unlicensed software and invited to utilize available software assets management (SAM) tools to conduct compliance audits on their software.

Despite a general lack of administrative capacity within the Ministry of Culture, BSA and the Copyright and Neighboring Rights Directorate maintained a fruitful and cooperative relationship in 2014. The

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Directorate successfully developed an administrative channel enforcement program during the year in an effort to substitute for the criminal channel enforcement efforts previously carried out by the police. The Directorate also resumed an end-user enforcement program involving enterprise end-user administrative inspections and cooperated with BSA on issuing warning letters. The Ministry of Culture, however, lacked the administrative capacity to meet the demands of various intellectual property rights holders.

Since June 2014, BSA has enjoyed the support of the Cyber Crime Unit's PDC2 (police direct contact) enforcement program as an alternative approach for successful enforcement and prevention of software-related crimes. The project was considered and approved by SANS in June 2014. By the end of the year a total of 159 protocols for warning and instructions were issued to local legal entities.

The Supreme Cassation Prosecution Office (SCPO) remained inactive on intellectual property in 2014. Only a few criminal cases have reached the trial stage, and none have reached final resolution. BSA recommends that the SCPO establish a long-term supervision program to monitor and analyze the work of particular prosecutors, observe the grounds for their motions to terminate or suspend criminal proceedings, and provide institutional guidelines and methodological support on how to investigate and prosecute intellectual property crimes. SCPO should cooperate with the private sector to address the chronic problem of prosecutors wrongfully terminating or refusing to initiate criminal proceedings for intellectual property offenses. The Attorney General's Office should maintain a sustained dialogue with the private sector, with ongoing high-level support from the SCPO, in keeping with the public-private cooperation it has exhibited in the past. The competent bodies should promptly complete an updated Manual for Uniform Prosecutors' Practices in Investigating and Prosecuting Intellectual Property Rights Crimes and circulate the manual as an Attorney General's mandatory instruction to district and regional prosecutors' offices.

Technical Assistance and Education: In 2014, BSA representatives participated in a variety of events and delivered presentations on the current legal framework and best practices in the investigation and prosecution of software crimes, including the OSAC Bulgaria Country Council Conference on Intellectual Property Rights and Brand Protection on June 17, 2014 and the anti-counterfeiting workshop "Meeting with the Judges" organized with the Bulgarian Patent Office on December 8, 2014.

Recommendation: Due to continuing high levels of unlicensed software use by enterprises, especially small- and medium-sized business, as well as concerns about the commitment of prosecutors to pursue much needed criminal enforcement actions, BSA recommends that USTR maintain Bulgaria on the **Watch List**.

GREECE

Due to the persistent and growing high levels of unlicensed software use both within the public and private sectors, insufficient enforcement activity, and the continuing need to implement policies to ensure that government agencies use only licensed software, BSA recommends that Greece remain on the Watch List.

Overview/Business Environment

The rate of unlicensed software use in Greece is among the highest levels for European Union (EU) members states, requiring urgent improvements to the legal framework in order to encourage the both the private and public sectors to procure and use properly licensed software.

Copyright

The rate of unlicensed software use in Greece has risen to 62 percent in 2013 (from 61 percent in 2011 and 58 percent in 2009). This represents a commercial value of US$220 million in unlicensed software.[1] The effects of this trend are fewer job opportunities and decreased revenues for local information and communication technology (ICT) businesses, further contributing to the huge financial problems faced by the country in recent years.

Government and State-Owned Enterprise Licensing/Legalization: The government of Greece should implement a policy requiring all government agencies to use properly licensed software. Consistent with government led working group discussions, this policy should assign the General Inspector of Public Administration with the responsibility of overseeing an audit of the government's use of software and developing of an awareness campaign to educate public officials about the risks associated with the use of unlicensed software. The General Inspector should also issue a circular providing that requests for proposal (RFPs) for public procurements include a clause establishing that the software publisher will have the right to perform audits of the bidder in order to verify compliance with the licenses of software in use. The adoption of effective, transparent, and verifiable software asset management procedures, where government agencies conduct regular audits of the software they have installed to ensure, among other things, that all software in use is properly licensed, could also provide a powerful positive example to private enterprise.

Statutory and Regulatory Provisions: BSA is following an ongoing consultation regarding proposed legislation that would establish a "Committee for the Communication of Copyright and Related Rights Online Infringements." The draft law would provide rights holders with an expedited process to obtain an order requiring the removal of infringing content or the disablement of access to the violating content. BSA welcomes the opportunity to participate in these consultations in order to ensure that the final legislative properly balances the interests of copyrights holders, users, and internet service providers.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

BSA also advocates for amendments to the relevant laws related to the certification of tax compliance by third party auditors. Specifically, BSA recommends that an assessment of whether firms obliged to undergo third party audits for tax compliance are also compliant with software licenses be included in the auditors' reports or the tax compliance certification.

Compliance and Enforcement: The Financial and Economic Crimes Unit (SDOE) conducted an increased number of *ex officio* inspections in Athens in 2014 compared to 2013. SDOE conducted around 25 raids during the first half of 2014. Unfortunately, due to an internal reorganization, the SDOE carried out significantly fewer inspections during the second half of the year. SDOE's 2014 raids resulted in the imposition of more than 130,000€ in administrative fines against infringers. As the only competent authority in Greece with a demonstrated record of pursuing software infringement cases, it is critical that the SDOE's Intellectual Property Rights (IPR) Department receive the funding and resources that it needs to carry out its mission. The SDOE requires additional trained personnel and, building upon the good work to date, should conduct more frequent inspections.

Inspections that were suspended due to SDOE's reorganization should be rescheduled as soon as possible. SDOE should also resume issuing letters to companies requesting inventories of software in use and associated licenses and invoices. In addition, SDOE should resume issuing follow-up warning letters in cases of non-responsive companies, and conduct inspections, when appropriate, against non-responsive companies. SDOE should readopt the practice of publishing the results of raids on its website and issuing public releases to raise public awareness. Furthermore, SDOE should more efficiently enforce the policy that inspectors check, in addition to tax compliance, software license compliance in daily tax inspections. Most importantly, SDOE should increasingly focus its efforts on large scale violators. Unfortunately, SDOE generally avoids investigating enterprises potentially using more than 50 illegal software products (i.e., larger enterprises), apparently to avoid triggering the legal threshold for criminal liability that would require initiating complicated and time consuming criminal investigations and prosecutions. This policy needs to change, and BSA urges SDOE to refocus its efforts to pursue large enterprises using unlicensed software.

BSA commends Greece for recent changes to its Code of Civil Procedure that have improved the efficiency and timeliness of civil infringement suits. While parties typically settle the cases out of court, the special intellectual property departments within the Civil Courts of First Instance of Athens and Thessaloniki, and within the Court of Appeals of Athens, are valuable tools for efficient and quality final judgments. BSA hopes to see this program extended to other cities in Greece.

On the other hand, BSA observes persistent problems with criminal enforcement in Greece. Criminal cases are beset with delays and in the rare instance that a defendant is ultimately convicted, courts are reluctant to issue adequately deterrent sentences and penalties.

Recommendation: Due to the persistent and growing high levels of unlicensed software use both within the public and private sectors, insufficient enforcement activity, and the continuing need to implement policies to ensure that government agencies use only licensed software, BSA recommends that Greece remain on the **Watch List**.

KAZAKHSTAN

Due to ongoing legislative and enforcement challenges, as well as Kazakhstan's high rate of unlicensed software use, BSA recommends that USTR places Kazakhstan on the Watch List.

Overview/Business Environment

The overall business environment for the software industry in Kazakhstan remained largely unchanged in 2014. According to the most recent data, the rate of unlicensed software use in Kazakhstan has was 74 percent in 2013. This represents a commercial value of US$136 million in unlicensed software.[1]

Copyright and Enforcement

BSA is primarily concerned about the significant number of commercial entities that persist in using unlicensed software.

BSA prioritizes two main legislative issues related to the use of unlicensed or under-licensed software. First, the Criminal Code provides police with *ex officio* authority to commence criminal copyright cases upon request from the intellectual property rights holder, but it is rarely used. Article 198 of the Criminal Code, establishing criminal liability for infringing intellectual property, has limited impact because it refers to the manufacturing and sale of illegal copies only. It is not clear whether the installation and use of unauthorized software constitutes a violation under this provision, the police are reluctant to initiate cases and conduct inspections and investigations against such enterprises.

Furthermore, the 2014 Presidential Decree imposing a moratorium for performing *ex officio* inspections against small- and medium-sized businesses (SMBs) effectively suspended all enforcement actions by the authorities against such entities. [2] This has made it very difficult for the rights holders to identify and prove intellectual property violations and pursue monetary claims against SMBs using unlicensed software in 2014. As a result the number of reported enforcement actions against enterprises infringing software copyrights dropped from 323 in 2013 to 51 in 2014.

Although the moratorium against inspections expired on January 1, 2015, the decree imposes a ban on holding regular *ex officio* inspections by enforcement bodies. The decree allows inspections only in response to requests from affected rights holders. The rights holder is now required to provide evidence of the unauthorized use, which is often difficult to obtain without assistance from state bodies, in order to initiate further inspections by the authorities.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[2] Decree of the President of the Republic of Kazakhstan on Fundamental Measures to Improve the Entrepreneurial Activity No. 757: February 27, 2014.

This situation, combined with vague and inefficient *ex parte* search provisions in the civil legislation, means that rights holders are now unable to undertake adequate and timely criminal or civil enforcement actions against enterprises using unlicensed or counterfeit software in their business activity.

Second, because of unclear provisions, the Normative Ruling of the Supreme Court dated December 25, 2007, No. 11 has been interpreted as prohibiting demands for compensation if an offender did not aim to sell counterfeit copies of software.[3] Such an interpretation is contrary to the provisions of articles 48 and 49 of the Law on Copyright and Related Rights, which provide for civil liability both for sale *and use* of unlicensed software. The provision has been amended in by the Normative Ruling of the Supreme Court dated December 24, 2014, No. 3, which will hopefully address this problem.

Government Licensing/Legalization: Establishing and implementing appropriate provisions to regulate the acquisition and management of software by the government is critical to ensuring the respect for intellectual property in Kazakhstan. The adoption of effective, transparent, and verifiable software asset management procedures, where government agencies conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed, could also provide a powerful positive example to private enterprises.

Recommendation: Due to ongoing legislative and enforcement challenges, as well as Kazakhstan's high rate of unlicensed software use, BSA recommends that USTR places Kazakhstan on the **Watch List**.

[3] Normative Ruling of the Supreme Court, no. 11 *On Application by the Courts of Certain Provisions of Legislation for the Protection of Copyright and Related Rights*: December 25, 2007.

REPUBLIC OF KOREA

Due to an increasingly difficult market access environment for information and communications technology (ICT) products and software and on-going concerns related to government use of unlicensed software, BSA recommends Korea be placed on the Watch List.

Overview/Business Environment

The overall commercial environment in the Republic of Korea (Korea) for BSA members, and the information and communication technology (ICT) sector as a whole, is mixed. Korea has a strong ICT market and a mature legal and enforcement system. Over the last several years, however, a number of policies have been adopted that have erected substantial market access barriers to foreign ICT products and software. Such policies include: local procurement preferences; local testing requirements; and requirements to comply with national technical standards even when commonly used international standards are available. Existing and proposed rules also threaten to increase the difficulty of providing cloud-based services to the Korean market, including by requiring local data storage and restricting the international flow of data in a manner inconsistent with Korea's international commitments.

Data suggest that the use of unlicensed software by enterprises is declining in Korea (see below). Nevertheless, BSA remains very concerned about persistent under-licensing of software in a variety of government agencies, which is inconsistent with Korea's commitments to the United States under the Korea-US Free Trade Agreement (KORUS FTA). Not only does this harm the legitimate commercial interests of BSA members, but it also raises potential security risks for the government agencies engaged in such activities. Additionally, there has been a general decline in the number of raids undertaken and there are signs that enforcement authorities are becoming increasingly reluctant to pursue cases against enterprises suspected of using unlicensed software, which threatens continued progress in reducing unlicensed software use in Korea.

Market Access

The adoption of procurement preferences for domestic firms and measures imposing additional regulatory burdens, often justified by security concerns, have decreased market access for BSA members in Korea. Additional proposed measures could further impose restrictions on BSA members interested in providing Internet-based services, such as cloud-services, in Korea.

Cross-Border Data Flows and Server Localization: The Financial Service Commission's (FSC) regulation on "Outsourcing of data processing and IT facilities of financial institutions" imposes severe restrictions on the movement of data to storage facilities outside of Korea. This regulation presents a major impediment to global ICT companies' cloud businesses and such polices undermine the benefits that a globally distributed infrastructure can provide to consumers, enterprises and small businesses around the world. It also appears to conflict with provisions under the KORUS FTA. Despite considerable efforts to raise these concerns to senior Korean and US government officials by the leadership of a wide range of industries, the FSC has not been receptive to relaxing the regulation.

For several years, the Korean government and now the Korean legislature is considering a so-called "Cloud Bill." The stated purpose of the bill is to promote economic growth through the development of the technology sector, and specifically to facilitate the development, deployment, and adoption of cloud services in Korea. BSA is reviewing the latest draft, but we have raised concerns about particular aspects of previous versions. For example, BSA argued against creating new cloud-specific regulatory and certification requirements for issues, such as security and privacy, that are much broader in scope than cloud computing. The bill also inappropriately classifies cloud-computing as a telecommunications service instead of an ICT service. While some of the bill's provisions remain unclear, we are also concerned about the possibility that the new law could impose server localization requirements or restrictions on cross-border data-flows, similar to our concerns described above. Thus far, the National Intelligence Service (NIS) has maintained the position that government agencies should not use commercial cloud services.[1] We are concerned that, even after enactment of the bill, this position will prevail and public agencies will be discouraged or prohibited from using commercial cloud services.

Discriminatory Security Certification Requirements Applied for Foreign IT products: Since 2011, the Korean government has imposed additional security verification requirements for international Common Criteria-certified information security products that are procured by Korean government agencies. However, no such requirement was required of locally-certified products. In 2014, the Korean government began imposing similar security-conformity testing requirements on international Common Criteria-certified networking products, not just information security products. This new policy came into effect in October 2014 for all central government agencies and is expected to be extended to all public organizations, local governments, and other government-related agencies, such as educational institutions, in 2015. These policies combined have been interpreted by Korean government agency procurement authorities as requirements to buy local products and to avoid foreign. While the Korean government has issued clarifications to government agencies, to date there has been no change in the implementation of these policies.

Korea, being a member of the Common Criteria Recognition Arrangement (CCRA), should recognize international certification from accredited laboratories and should not impose further requirements for certified products. The additional requirements are not consistent with the spirit of CCRA, which is to "eliminate the burden of duplicating evaluation of IT products and protection profiles." To make matters worse, a separate conformity testing is required for each government agency, even if it is the same product that has been procured and verified for another government agency.

This discriminatory application of security testing in public procurements to only international information security products also appears inconsistent with Korea's international commitments to national treatment and non-discrimination.

Procurement Preferences: In addition to the standards and certification related issues described above, BSA members are also concerned about other preferences established or proposed in Korea's public procurement regime. We urge Korea to avoid adopting procurement preferences based on particular forms of technology or licensing models for software, which could also conflict with Korea's international commitments. Instead, Korea should adopt a technology neutral approach that evaluates whether a product or service provides the requested functionality and required quality at a competitive

[1] The NIS issued an official directive to other government agencies in February 2012. As a result of this directive, all national universities and some government agencies have suspended use of commercial cloud services.

price. It is important for procurement officials to consider the entire life-cycle costs of a software solution or technology, rather than focusing on the upfront license fees or purchase price.

The current administration has adopted a number of policies to promote small- and medium-sized enterprises (SMEs). In that context, we understand that there is a pending proposal to designate a large number of IT products and software categories (system software, application software, computer programming services and computer system integration) as an "SME-designated sector." If so designated, we understand that certain public procurement requests under a certain threshold would be required to go to SME suppliers. We urge the Korean government to avoid such procurement preferences, which would not only unfairly impact BSA members, but more importantly, may deprive Korean public entities from buying or licensing the best possible solutions available.

Copyright and Enforcement

The rate of unlicensed software use in Korea has continued a slow but steady decline. According to the latest data, 38 percent of software used in Korea is unlicensed. That equates to a market value of US$712 million in unlicensed software.[2] While this figure is below the regional and global average for unlicensed software use, it remains relatively high when compared with comparable economies in the region and around the world.

Government and SOE Licensing/Legalization: Government use of illegal software remains a serious problem. Frequently government agencies purchase fewer licenses than required and used because of budgetary concerns, even though the cost of software to government may be much lower than the rates offered to enterprises. Unfortunately, the government has been resistant to taking the necessary and effective steps, and sustaining them to solve this problem. After considerable effort, the Ministry of Defense addressed this issue, but unfortunately, this effort is not being replicated by other ministries, such as the Ministry of Interior and others, where unlicensed software continues to be an issue. BSA requests that USTR open up a dialogue with relevant representatives of the Korean government to identify a mechanism to address this challenge and to ensure Korea's full compliance with its commitments under the KORUS FTA.

Compliance and Enforcement: Criminal enforcement has been an effective mechanism for BSA members to protect their rights and fight against the use of unlicensed software by enterprises in Korea. The police, prosecutors' offices and the special judicial police under the Ministry of Culture, Sports and Tourism are the authorities primarily involved in enforcement activities against enterprises using unlicensed software.

The special judicial police are specifically tasked with investigations and inspections concerning copyrights and they are relatively active in conducting enforcement activities against software copyright infringers. This force, however, has limited resources and BSA members also rely on the enforcement actions of the police.

[2] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Unfortunately, BSA has observed an alarming trend, in which the number of criminal enforcement actions undertaken by the law enforcement authorities has dropped precipitously over the last several years. According to BSA's information, the total number of criminal actions taken in 2014 dropped by approximately 25 percent when compared to 2013 and is less than 50 percent of the numbers seen in 2010. One problem in this regard is that prosecutors and courts are applying overly stringent requirements for initial proof of illegal use to issue warrants. This trend is in stark contrast to the Korean government's stated objectives of reducing the rate of unlicensed software use to less than 20 percent by 2020. BSA recommends that Korean law enforcement authorities commit to a minimum number of criminal enforcement actions not less than the average number taken between the years 2010-2012.

As criminal enforcement has become increasingly difficult, BSA members have increasingly turned to civil litigation. BSA members have found that the civil courts are not very effective in addressing software copyright infringement cases. For example, although preliminary injunctions are available they are not often exercised, it is difficult to acquire evidence, and damages awarded tend to be too low to compensate the rights holders or to send a deterrent signal against future infringements.

Recommendation: Due to an increasingly difficult market access environment for ICT products and software and on-going concerns related to government use of unlicensed software, BSA recommends Korea be placed on the **Watch List**.

We note that the USG has an active dialogue on KORUS implementation and the issues raised herein should also be included in that dialogue. In addition, we note that Korea is keenly interested in the Trans-Pacific Partnership negotiations. It is incumbent upon the Administration to ensure that existing agreements are honored as the US government reviews potential eligibility criteria.

MEXICO

Although Mexico has emerged as a leader in promoting effective software asset management in the public sector and has provided tremendous support in administrative enforcement, persistent concerns about unlicensed software use by enterprises and on-going concerns regarding judicial enforcement mechanisms lead BSA to recommend that Mexico be maintained on the Watch List.

Overview/Business Environment

The rate of unlicensed software use has declined over the last several years, but unauthorized or counterfeit software remains available in most street markets, including Plaza de la Computación, Plaza del Videojuego, Plaza Meave, Tepito, San Juan de dios, la Cuchilla, and other notorious markets, both physical and on-line. The government of Mexico should be commended for adopting software asset management procedures in certain government agencies that comport with international best practices.

Copyright and Enforcement

The primary concern for BSA remains the unlicensed use of software by enterprises. The most recent information indicates that the rate of unlicensed software in Mexico is 54 percent, representing an estimated commercial value of unlicensed software of US$1.2 billion.[1] Illegal software is also commonly available at street markets ("carpeteros"), from online auction sites, and by download through specialized file-sharing sites. In addition, "white box" vendors (small local assemblers or non-brand name vendors of computer hardware) continue to be a considerable source of unlicensed software.

Enterprise Licensing/Legalization: Enterprise under-licensing of software is a significant problem in Mexico. It is common to find companies that share the same software licenses.

Government Licensing/Legalization: Ensuring that government agencies buy and use only legal software according to their licenses is an on-going effort for all governments. Mexico has been a leader in world in terms of adopting transparent and verifiable software asset management (SAM) procedures in various government agencies. The Ministry of Economy and its component agencies were the first government agencies in the world to obtain a Verafirm Certification, which confirms that an organization's SAM practices are aligned with the ISO19770-1 SAM standard. The Mexican Tax Administration (SAT) is the largest entity ever to have obtained a Verafirm certification. The Mexican Institute of Industrial Property (IMPI) is the first patent office in the world to be Verafirm certified. Now the Ministry of Economy is exploring the possibility of implementing a voluntary audit system for procurement processes.

The award of Verafirm certifications to SAT, IMPI and other agencies has inspired private and public sector entities to voluntarily legalize. To build on this momentum, the Federal Government should

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

conduct random audits of government contractors or suppliers, to guarantee that they are using legal software.

Compliance and Enforcement: IMPI's efficacy and quality of legal analysis, as well as a clear improvement in inspection practices, has represented a very positive development in the enforcement of BSA member intellectual property rights. Legal criteria are clearer and enforcement practices are more effective. Outreach campaigns launched by IMPI, such as the Expo-Ingenio national tour have raised awareness regarding innovation and intellectual property. IMPI precautionary measures have become increasingly effective and constitute a deterrent. 1,509 IMPI actions were brought against enterprises using unauthorized software (1,059 *ex officio* actions and 450 *ex parte* raids and proceedings, also known as "full raids").

Beyond IMPI raids, significant hurdles and challenges stand in the way of creating a truly effective enforcement system. Copyright certificates are still required in administrative and criminal cases. Regional IMPI offices do not yet have enforcement inspectors. A typical intellectual property case brought to court is likely to take 10 years or more before a final decision is rendered. Judicial procedures need to be shorter, and fewer opportunities to continuously review due process issues over and over again.

Notorious markets are well identified, but stronger actions need to be taken against them. Online infringement is difficult to address because of the lack of basic investigative and prosecutorial tools, slow investigation processes, and IMPI and the Attorney General's Office (PGR) lack sufficient powers to gather evidence quickly and take down allegedly infringing products.

Criminal enforcement is not a practical method for enforcing against enterprise use of unlicensed software in Mexico. The requirement to have expert opinions for every case, as well as to provide physical copies of legal and illegal software makes criminal prosecution complicated. Police authorities normally argue that they have more important crimes to investigate.

Technical Assistance and Education: During 2014, BSA conducted training programs for a wide range of individuals, from IMPI officers, PGR officers, Customs inspectors, Federal Attorney's Office of Consumer (PROFECO) inspectors, judges and magistrates, to CPAs, chambers and associations, entrepreneurs, students, customs agents, importers, and exporters. The program topics included intellectual property, software protection, innovation, cyber security, ISP liability, software related tax matters, Verafirm certification, customs enforcement, licensing, administrative practices, notorious markets, rule of law, and accounting practices.

Recommendation: Although Mexico has emerged as a leader in promoting effective software asset management in the public sector and has provided tremendous support in administrative enforcement, persistent concerns about unlicensed software use by enterprises and on-going concerns regarding judicial enforcement mechanisms lead BSA to recommend that Mexico be maintained on the **Watch List**.

SOUTH AFRICA

Due to concerns about proposed government procurement policies that would discriminate against certain forms of software, and continuing challenges in addressing the use of unlicensed software by enterprises, BSA recommends that USTR identify South Africa as a Watch List country.

Overview/Business Environment

Despite having the most advanced intellectual property system in the region, the overall business environment in South Africa continues to concern BSA members.

Intellectual Property and Enforcement

BSA continues to monitor developments relating to the implementation of a Draft National Policy on Intellectual Property (Draft IP Policy), first published by the Minster of Trade and Industry and opened for consultation in 2013. The Draft IP Policy makes recommendations for a number of proposed reforms to South Africa's intellectual property system with the ultimate goal of creating economic opportunities and promoting innovation. BSA is concerned that elements of the Draft IP Policy may harm the development of a competitive marketplace in South Africa by undermining key protections for the software sector. BSA is particularly concerned about recommendations in the Draft IP Policy relating to the government procurement of software that would establish unhelpful preferences for specific software licensing models instead of allowing government bodies to choose from the vast range of technology choices that exist in the market.

Enterprise Licensing/Legalization: Unlicensed use of software by enterprise remains a significant problem for BSA members in South Africa. The latest data indicates that 34 percent of the software used in South Africa is unlicensed, with a value of US$385 million.[1]

Compliance and Enforcement: BSA members face challenges enforcing against the use of unlicensed software by enterprises. Police, prosecutors, and trial court judges often lack the training necessary to effectively work on cases involving complex intellectual property crimes.

Civil remedies, in particular, are ineffective as a means for addressing enterprise use of unlicensed software. Rights holders are deterred from bringing cases because in many circumstances, trial judges have insufficient knowledge regarding copyright and tend to issue insufficient damage awards.

Criminal enforcement against unlicensed software can be an effective means of enforcing against enterprises using unlicensed software. When criminal cases are prosecuted, South African law provides for effective criminal remedies. The effectiveness of such cases, however, often depends on the availability of a trained prosecutor to oversee the case.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Recommendation: Due to concerns about proposed government procurement policies that would discriminate against certain forms of software, and continuing challenges in addressing the use of unlicensed software by enterprises, BSA recommends that USTR identify South Africa as a **Watch List** country.

THAILAND

Due to on-going concerns regarding the level of unlicensed software use by enterprises in Thailand, as well as concerns about the implementation of security-related legislation now pending that may undermine the operations of BSA members, BSA recommends Thailand for the Watch List.

Overview/Business Environment

Thailand's software market did not significantly improve in 2014 due mainly to the persistence of high rates of unlicensed software use by enterprises. This is exacerbated by the widespread use of unlicensed software in the public sector.

The Royal Thai Government (RTG) lacks clear goals and strategies to reduce unlicensed software use by enterprises (both businesses and government agencies) and has failed to set a good example to Thai businesses. The copyright amendment bill, enacted in 2014, was a missed opportunity to meaningfully improve the legal mechanisms to prevent the use of unlicensed software by enterprise. Instead, the bill includes broad exceptions and insufficient protections for rights management information (RMI) and technological protection measures (TPM) which BSA members use to deter unauthorized and illegal use of their products and services. It remains unclear whether the bill amending the Computer Crime Act will include crimes related to intellectual property.

BSA is also concerned that fair and equitable market access for our members' products and services could be harmed if legislation regarding personal data protection and cyber security remains both vague and potentially over-prescriptive. BSA urges the RTG to conduct an open and transparent process when developing these and other pieces of legislation, soliciting the input of interested stakeholders including BSA members, and taking into consideration industry views before such legislation is presented to the national legislative body.

Market Access

BSA shares the goals of the RTG's Digital Economy initiative and supports the thoughtful enactment of necessary legislation regarding privacy and cyber security. Before finalizing such legislation, however, the RTG should minimize unintended effects that will harm the ability of BSA members and others technology sector to provide innovative and effective information and communications technology (ITC) products and services, including software.

Security: The draft national cybersecurity bill, approved in principle by the Thai Cabinet on January 6, 2015, is designed to strengthen the cybersecurity capabilities of government agencies and provide appropriate breach notification procedures. The draft, however, raises concerns because the Office of the National Cybersecurity Committee would have broad powers to access confidential and sensitive information, without sufficient protections to appeal or limit such access. Granting the Office of the National Cybersecurity Committee such broad powers will undermine public confidence and trust in information technology generally and harm the ability of BSA members to provide the most innovative and effective software solutions and services to the market.

Privacy: The draft Personal Information Protection bill, also approved in principle by the Thai Cabinet on January 6, 2015, is designed to build public trust and confidence in ITC products and services and to implement the APEC Privacy Framework's principle of cross-border data transfer. BSA filed comments on the draft legislation in September 2014, highlighting the importance of the protection of personal information and the prevention of misuse of such information for fostering trust and confidence in the digital environment. At the same time, BSA noted that the bill contained imprecise or unclear provisions in some cases, and in others appeared to take an overly prescriptive approach not taking into adequate consideration the nature of the personal information in question. Such an approach does not take into account the expected evolution of digital products and services and could result in undermining both the effective protection of personal information and the trust and confidence that are necessary for wide adoption of digital products and services in the economy.

Copyright and Enforcement

BSA has enjoyed good cooperation from the RTG authorities including the Economic Crime Division in addressing software piracy in Thailand in 2014. Civil and criminal penalties awarded against enterprises found to be using unlicensed software are generally appropriate. The latest figures, however, indicate that rate of unlicensed software use was 71 percent in 2013, representing a commercial value of US$869 million.[1] The rate of unlicensed software use in Thailand is well above the Asia regional average of 62 percent indicating that there is still much progress to be made. Beyond enterprise use of unlicensed software, the failure to fully implement the existing cabinet resolution on legal software use, procurement, and installation in the public sector remains a problem for BSA members.

Statutory and Regulatory Provisions: The RTG enacted a copyright amendment bill in 2014. BSA had filed comments on the bill in 2013, and again in September 2014 when the bill was reintroduced (with few if any changes). Unfortunately, BSA's comments, which raised concerns about particular provisions and suggested amendments, were not taken into serious consideration. BSA is disappointed that the bill fails to provide effective remedies against the trafficking and distribution of devices and technology designed for the purpose of circumventing TPM. We are also concerned about the inclusion of overbroad or unnecessary exceptions, including for the deletion or alteration of RMI. Onerous requirements on the copyright owner to prove the intent or knowledge of one suspected of deleting/altering RMI or circumventing TPM will only hamper efforts to enforce against this activity. Finally, we are concerned that the law may lead to an application of the first sale doctrine that does not respect the terms of software licensing agreements with respect to the resale or reproduction of software. BSA looks forward to working with the RTG to mitigate and address these deficiencies in implementing regulations and future revisions of the current copyright law.

BSA hopes that the pending draft amendment to the Computer Crime Act, which the Thai Cabinet approved in principle on January 6, 2015, will present an opportunity to address Internet-based software infringement by explicitly adding intellectual property crimes to the scope of that law. The RTG should ensure that there is an open and transparent process for stakeholders to provide meaningful input before the bill is presented to the legislative body.

[1]Data on unlicensed software installation rates and commercial values are taken from the 2013 BSA Global Software Survey at www.bsa.org/globalstudy. This survey is conducted every other year for BSA by IDC, which this year polled computer users in 34 markets including nearly 22,000 consumer and business PC users and more than 2,000 IT managers.

Compliance and Enforcement: Thailand has a specialized intellectual property court, which has improved the effectiveness of intellectual property litigation. Occasionally, damages awarded in civil litigation are reasonable, although award amounts are quite inconsistent. Expenses are awarded but only very small amounts and do not cover the actual costs. Preliminary injunctions are not sufficiently available to be an effective tool. In addition, criminal cases can be effective in Thailand, but the courts should apply more deterrent penalties for convictions.

Government Engagement: BSA has developed positive relationships with the Electronic Transaction Development Agency (ETDA), which is one of the leading agencies tasked by the Prime Minister to oversee the implementation of the Thai Digital Economy initiatives, and regularly engages with ETDA officials regarding policies of mutual interest.

Technical Assistance and Education: On November 6, 2014, BSA conducted a training program on software asset management (SAM) for approximately 150 government officials attending a Ministry of Information and Communication Technology (MICT) seminar. The training improved officials' understanding of basic practices to prevent the use of unlicensed software. BSA provided its online SAM course, a program which helps organizations understand and implement the principles of the International Standards Organization (ISO) 19770-1 SAM standard. BSA has sponsored a government agency to become Verafirm Certified, which confirms that an organization's SAM practices are aligned with the ISO19770-1 SAM standard. If the agency clears this certification requirement, it will become the first entity in Thailand to receive Verafirm Certification.

Recommendation: Due to on-going concerns regarding the level of unlicensed software use by enterprises in Thailand, as well as concerns about the implementation of security-related legislation now pending that may undermine the operations of BSA members, BSA recommends Thailand for the **Watch List**.

TURKEY

Based on Turkey's failure to implement policies to ensure that government agencies use only licensed software and persistent high levels of unlicensed software use by enterprises, BSA recommends that Turkey be maintained on the Watch List.

Overview/Business Environment

With an economy that fared remarkably well over the past decade despite recessions in Europe and other parts of the world, Turkey is an important emerging market for the software industry. Despite the overall health of the economy, the software market continues to underperform due to unacceptably high levels of unlicensed software use by enterprises and public entities.

Copyright and Enforcement

The key concern in Turkey remains the widespread use of unlicensed software by enterprises. The most recent data indicate that the unlicensed software rate in Turkey is 60 percent, representing a commercial value of unlicensed software of US$504 million.[1]

Government and SOE Licensing/Legalization: In 2008, the Turkish Government issued a circular that ostensibly requires all government agencies to ensure the use of properly licensed software.[2] Nearly seven years later, the government of Turkey has yet to truly implement the circular. As a consequence, unlicensed use of software within the government and in state-owned enterprises (SOEs) remains rampant. In 2015, Turkey should allocate the budget and resources necessary to ensure that each ministry and public authority issue and adhere to similar circulars to establish reasonable software legalization procedures. The adoption of effective, transparent, and verifiable software asset management procedures, where government agencies and SOEs conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed, could also provide a powerful positive example to private enterprises. The government should also conduct public awareness campaigns to highlight the risks associated with using unlicensed software, such as the potential exposure to security vulnerabilities, and the collateral harms to domestic innovation and the growth of the information and communications technology (ICT) industry.

Statutory and Regulatory Provisions: Turkey has been developing draft amendments to the Law on Intellectual and Artistic Work for the past several years. BSA encourages Turkey to develop these amendments in an open and transparent consultation, in which all interested stakeholders are afforded meaningful opportunities to participate and provide input.

Compliance and Enforcement: Enforcement against unauthorized use of software by enterprises improved in 2014. BSA brought 90 civil and criminal actions (up from 80 in 2013).

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[2] *Circular on Legalization of Software Use in Public Entities*, No. 2008/17 (July 2008).

Turkey's criminal justice system provides an effective forum for intellectual property enforcement. Law enforcement authorities maintain units specialized for intellectual property enforcement that have served as capable partners in the fight against the distribution and use of unlicensed software, and prosecutors are willing to take on intellectual property infringement cases. The system, however, could be further improved by encouraging judges to issue deterrent sentences and damage awards in criminal and civil cases, respectively. Although courts generally provide adequate equitable relief (e.g., orders requiring seizure or destruction infringing goods), they have been reluctant to issue adequately deterrent awards and penalties to defendants in both civil and criminal cases.

Recommendation: Based on Turkey's failure to implement policies to ensure that government agencies use only licensed software and persistent high levels of unlicensed software use by enterprises, BSA recommends that Turkey be maintained on the **Watch List**.

Countries of Concern

AZERBAIJAN

Since the Government of Azerbaijan has failed to provide adequate enforcement against unlicensed use of software intellectual property and has failed to make meaningful progress in improving intellectual property laws and policy, BSA is highlighting Azerbaijan as a Country of Concern.

Overview/Business Environment

At 85 percent, the rate of unlicensed software use in Azerbaijan continues to be one of the highest in the world. This represents a commercial value of unlicensed software of US$103 million.[1]

Intellectual property enforcement in Azerbaijan is deficient and intellectual property protection is not a priority for the government. While the general public and government officials in Azerbaijan continue to gain a better understanding of the risks involved in using unlicensed software and the importance of intellectual property to the economy, in practice policies have not changed. BSA Members have undertaken extensive, substantive work to ensure the software distribution channel is free from unlicensed software, but a major intellectual property enforcement vacuum remains with respect to commercial enterprises, large corporations and small- and medium-sized enterprises (SMEs) alike, which continue to use unlicensed software.

Copyright and Enforcement

BSA urges the government of Azerbaijan to take steps to improve its relevant laws governing the protection and enforcement of intellectual property and to ensure that they are in compliance with international standards. Specifically, Azerbaijan should amend:

- the Criminal and Administrative Procedural Codes to provide *ex officio* authority to law enforcement agencies and to increase penalties for intellectual property infringements to create an effective deterrence against the use of unlicensed software;
- the Civil Code to provide *ex parte* search provisions for effective enforcement against commercial end-users; and
- the Civil Code, the Law on Copyright and Related Right and the Law on Ensuring Intellectual Property and Combating Piracy to provide for deterrent damages awards.

Recommendation: Since the Government of Azerbaijan has failed to provide adequate enforcement against unlicensed use of software intellectual property and has failed to make meaningful progress in improving intellectual property laws and policy, BSA is highlighting Azerbaijan as a **Country of Concern**.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

MALAYSIA

Due to both positive developments and continuing concerns regarding the unlicensed use of software by enterprises, BSA is recommending Malaysia as a Country of Concern.

Overview/Business Environment

There were no major changes to the intellectual property and market access policy environment in Malaysia in 2014. As business models continue to migrate to online and mobile platforms, the Malaysian government should correspondingly adjust its attention through adequate devotion of resources, training, and redirection of its enforcement efforts to target and speed investigations and prosecutions against all forms of unlicensed software use, especially by corporate end-users.

Copyright and Enforcement

The latest data available from the BSA Global Software Survey, released in June 2014, indicated that the rate of unlicensed use of software is Malaysia is 54 percent. This represents a commercial value of US$616 million in unlicensed software.[1]

Enterprise Licensing/Legalization: The use of unlicensed software by enterprises continues to be the main threat to the software sector. Certain cities or regions have higher loss of sale of software products and services due to unlicensed software use, especially the developed areas and major cities (i.e. Kuala Lumpur, Penang, and Johor Bahru) which have a higher concentration of enterprise end-users.

Government and Enterprise Licensing/Legalization: In order to address the unlicensed use of software by government agencies and state-owned enterprises (SOEs) more effectively, BSA continues to call for mandatory annual software audits of enterprises and Malaysian government agencies, with results filed with the Companies Commission of Malaysia and the Enforcement Division of the Ministry of Domestic Trade, Co-operatives and Consumerism (MDTCC). Establishing and implementing appropriate provisions to regulate the acquisition and management of software by the government is critical to real success. The adoption of effective, transparent, and verifiable software asset management procedures, where government agencies conduct audits of the software they have installed to ensure, among other things, that all copies in use are properly licensed, could also provide a powerful positive example to private enterprises. The government should also conduct public awareness campaigns to highlight the risks of unlicensed software use, from the exposure to security vulnerabilities and malware to the damage caused to creativity and innovation and the growth of the information and communications technology (ITC) industry.

Compliance and Enforcement: BSA and its members conducted almost 80 criminal end-user actions in 2014, up from 60 criminal actions in 2013. Similar to recent trends, most of the companies recently

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

inspected are under-licensed as opposed to having no licenses at all, which is a positive sign of increasing copyright awareness.

Enforcement of copyright is primarily conducted by MDTCC and it is relatively efficient. In our experience, although the Royal Malaysia Police have the powers of enforcement under the Copyright Act of 1987, they are only concerned with intellectual property infringements perpetrated by criminals involving high volume distribution and/or manufacturing of physical pirated copies.

Nevertheless, there is a backlog of cases in the judiciary. Most of the backlog is attributable to the lack of resources for investigations and prosecutions. More resources should be expended on capacity building to train investigators and prosecutors on intellectual property cases. Similarly, the Malaysian government should assign more dedicated judges to the criminal intellectual property courts, and establish the promised 15 sessions courts (with intellectual property specialists) around the country to reduce backlogs and obtain convictions that will be publicized in the media as a form of deterrence. In addition, training efforts to sensitize the judiciary as well as prosecutors on the serious nature of intellectual property infringements should be conducted.

Holographic Label Requirement (Proposal to Review): BSA recommends that the government of Malaysia should review and repeal the labelling requirement, which requires manufacturers and distributors to affix holographic labels/stickers on all copies of works on optical discs (e.g., DVDs, CD-ROMs, etc.).[2] The requirement has not been enforced and the problem it is designed to remedy, optical disk piracy, is less of an issue as consumers increasingly acquire unauthorized copies of copyrighted works online. The labelling requirement now serves only to impose unnecessary financial and administrative burdens on rights owners.

Government Engagement: BSA has consistently engaged with the Malaysian government to improve the effectiveness of enforcement and compliance initiates. BSA appreciates the efforts of the US Embassy in Malaysia, which works with representatives of a variety industries reliant on intellectual property. The Malaysian government seriously considers the recommendations of the US Embassy and the representatives of industries that rely on intellectual property protection, including BSA members, resulting in meaningful improvements in the intellectual property laws (e.g., the imposition of statutory damages for civil infringement under the copyright laws).

Technical Assistance and Education: BSA recommends that the Government of Malaysia conduct public awareness campaigns to highlight the harm caused by the use of unlicensed software, including the following:

1) establish awareness and training programs targeted at directors and senior management of companies, enlisting the support of the Kuala Lumpur Stock Exchange and the Companies Commission of Malaysia;
2) develop educational programs to reach out to secondary and University students on the importance of protecting intellectual property; and
3) develop awareness programs to educate consumers and members of the public on the risks of using unlicensed software.

[2] Ministry of Domestic Trade, Cooperatives and Consumerism Orders: Trade Description (Original Label) Order 2002 and Trade Descriptions (Optical Disc Label) Order 2010.

Recommendation: Due to both positive developments and continuing concerns regarding the unlicensed use of software by enterprises, BSA is recommending Malaysia as a **Country of Concern**.

MOLDOVA

Due to the lack of meaningful intellectual property enforcement for software in Moldova, BSA is highlighting Moldova as a Country of Concern.

Overview/Business Environment

The protection of intellectual property is simply not a priority for the government. As a consequence, there is no legal deterrence for commercial enterprises using unlicensed software, which exposes them to security vulnerabilities as well. The software industry enjoys a positive working relationship with the Intellectual Property Division within the Police General Inspectorate and the IT and Cybercrimes Section within the General Public Prosecutor's Office. In practice, however, the police lack sufficient resources, equipment, and expertise to effectively conduct inspections.

Copyright and Enforcement

Compared with other countries in the region, there are insufficient law enforcement inspections, criminal cases and convictions. The Ministry of Internal Affairs approved an internal reform strategy intended to improve intellectual property enforcement, but more concrete action is needed to address the exceedingly high rate of unlicensed software use, and the rapidly growing instances of unauthorized downloads of software. In 2013, the government restructured the police forces and created the Intellectual Property Division (IPD), which is intended improve intellectual property enforcement.

Intellectual property-related court proceedings are excessively lengthy. As a result, the software industry cannot secure effective enforcement. The process to obtain a civil injunction against an enterprise using unlicensed software takes longer than six months, compared to three days to three weeks in other jurisdictions in the region.

In order to improve intellectual property enforcement, law enforcement agencies need to significantly increase the overall number and size of actions against enterprises suspected of using unlicensed software. BSA urges the government to enter into joint public awareness campaigns with rights holders in order to raise awareness within commercial enterprises of both the legal and security risks associated with unlicensed software.

Recommendation: Due to the lack of meaningful intellectual property enforcement for software in Moldova, BSA is highlighting Moldova as a **Country of Concern**.

NIGERIA

Due to proposed guidelines that, if adopted, would make Nigeria one of the most restrictive and closed markets for ICT hardware, software and services, BSA recommends Nigeria as a Country of Concern.

Overview/Business Environment

As the largest economy in Africa, Nigeria presents significant opportunities for global information and communication technology (ICT) companies. The country's ICT industry has great potential to develop and grow if the government makes policy choices that enable it to integrate with the global digital economy. To that end, the Nigerian government has made ICT-enabled growth a top priority and is actively seeking to build a viable, domestic ITC and telecommunications sector.

In 2014, the Nigerian government released the Guidelines for Nigerian Content Development in Information and Communications Technology (Guidelines). If these guidelines are implemented, Nigeria would become one of the most restricted and closed ICT markets in the world. Specifically, the Guidelines impose stringent local content requirements for ICT hardware, software, and services for government and private sector procurements, restrict employment of non-Nigerian citizens in the sector, force technology transfer, require the disclosure of source code and other sensitive design elements as a condition of doing business, and impose severe data and server localization requirements.

The requirements in the Guidelines have been described as mandatory but it is unclear how the Jonathan government or a new All Progressives Congress (APC) administration (should APC win the impending national elections) will enforce compliance with the Guidelines. The severity of the Guidelines and the negative precedent they set to the region and globally warrant significant attention for the US government in the meantime.

Market Access

Cross-Border Data Flows: The Guidelines impose severe cross-border data and server localization requirements that would impact a wide range of sectors. Section 12.1.4, for example, requires ICT companies to "host all subscriber and consumer data" locally. Section 14.1.3 calls for all government data to be hosted "locally inside the country" within 18 months of the Guidelines' publication and Section 14.3.1 calls for the government to support local "data hosting firms" and to establish "appropriate service level requirements and standards for data service provisioning…"

Procurement: The Guidelines impose significant local content requirements for ICT hardware, software and services. Section 10.1 requires manufacturers to obtain certification that ICT hardware has been assembled in Nigeria and requires that 50 percent of "local content either directly or through outsourcing to local manufacturers." These requirements are not limited to ICT hardware – Section 11.4 requires local sourcing of software and directs government agencies to "carry out risk-based due diligence to identify…potential adverse impacts that may arise from using software…conceptualized and developed outside of Nigeria."

Importantly, these local content and sourcing requirements apply to both government and private sector procurements, violating the WTO's fundamental principle of national treatment: that imported and locally-produced goods must be treated equally once those imported goods have cleared the border.

Security: The Guidelines contain problematic requirements from both a business/competitive and security perspective. Section 11.3.1 can be interpreted to require multinational companies to reveal sensitive design elements, such as source code. Specifically, it requires multinational companies to "sign affidavits about the origin, safety, source and workings of software" being sold in Nigeria in order to "ascertain the full security of the product and protect national security." Section 11.4.5 further requires "assurances of the full security of source code." This extremely sensitive and proprietary information is at the core of ICT companies' products and the compromise of such information would severely harm their continued commercial viability.

The requirement to disclose sensitive information regarding a vendor's software is not imposed on domestic Nigerian companies. Consequently, it would create serious challenges for foreign companies to be able to operate or sell in Nigeria and would diminish the availability of foreign-made leading-edge software for Nigerian customers.

Copyright and Enforcement

According to the latest information, the use of unauthorized software in Nigeria stands at 81 percent, far above the regional and global average. This represents a commercial value of US$287 million in unlicensed software.[1] BSA urges the government of Nigeria to work with effected stakeholders to take effective steps to address this situation.

Recommendation: Due to proposed guidelines that, if adopted, would make Nigeria one of the most restrictive and closed markets for ICT hardware, software and services, BSA recommends Nigeria as a **Country of Concern**.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

PHILIPPINES

Despite positive developments, due to continuing concerns regarding the high rates of unlicensed use of software by enterprises, BSA is recommending the Philippines as a Country of Concern.

Overview/Business Environment

The business environment in the Philippines is improving. The copyright amendment bill that was passed in March 2013 paved the way for inspections by the Intellectual Property Office of the Philippines (IPO). Software companies continue to utilize IPO inspections as a key tool to support of enterprise software legalization.

Copyright and Enforcement

The latest information shows that the rate of unlicensed software use in the Philippines was 69 percent in 2013. This represents a commercial value of US$444 million in unlicensed software.[1] Enterprises engaged in the use of unlicensed software are concentrated in the metropolitan areas (Metro Manila, Metro Cebu and Metro Davao) and in economic zone areas (PEZA).

Government Licensing/Legalization: Memorandum Circular (MC) No. 115 dated April 5, 1999 mandates the use of only licensed software and applications in government offices. The circular is valid and binding among government offices. Establishing and implementing appropriate provisions to regulate the acquisition and management of software by the government is critical to real success.[2] The adoption of effective, transparent and verifiable software asset management procedures, where government agencies conduct audits of the software they have installed to ensure, among other things, that all copies in use are properly licensed could also provide a powerful positive example to private enterprises.

Statutory and Regulatory Provisions: Strengthening the legal and policy infrastructure is one of the strategic goals in the IPO's 2012-2016 Action Plan on IPR Protection and Enforcement. Below are some of the significant laws passed which have had an impact on intellectual property protection and enforcement:

Republic Act No. 10372 amending the Intellectual Property Code of the Philippines: These provisions took effect on March 22, 2013. Important amendments include:

- Granting enforcement and inspection powers to the IPO;
- Amending the provision on copyright infringement to include secondary liability; and

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[2] The government could consider revising the Government Procurement Act (Republic Act 9184 dated 10 January 2003), and/or its Implementing Rules and Regulations, to ensure that government entities are forbidden from purchasing illegitimate software and that only suppliers of legitimate software are permitted to participate in government procurement processes.

- Imposing a maximum penalty or doubling the amount of damages awarded when copyright infringement is committed by someone who circumvents technological protection measures or removes or alters electronic rights management information from protected works.

Republic Act No. 10365 amending Republic Act No. 9160, known as the Anti-Money Laundering Act (AMLA): Intellectual property violations are now one of the predicate offenses for violations under this law. Thus, property or proceeds from intellectual property violations may now be subject to a seizure order that the Court of Appeals may issue upon an *ex parte* verified petition by the Anti-Money Laundering Council (AMLC).

Compliance and Enforcement: Criminal enforcement is an effective means of enforcing against the use of unlicensed software by enterprises in the Philippines. The trial of cases in the lower courts, however, needs to be expedited. In addition, the courts have been hesitant to award penalties and damages sufficient to have a deterrent effect in intellectual property cases.

BSA members' relationships with enforcement authorities continue to improve. The National Bureau of Investigation (NBI), the Philippines National Police (PNP) and IPO have been very helpful in the software industry's enforcement and other campaigns. BSA members usually work with the NBI when it comes to software infringement. When conducting enforcement operations in other regions, BSA members often coordinates with local PNP officials.

Government Engagement: The IPO is approachable when it comes to private sector collaboration, in addition to enforcement. This continued approachability and responsiveness to requests from the private sector has contributed to improvements in the intellectual property protection and enforcement environment in the Philippines.

Technical Assistance and Education: BSA applauds the IPO's efforts, including the partnership with the Philippine Judicial Academy (PhilJA), to continuously provide seminar-workshops on rules and procedures, as well as substantive law and jurisprudence on intellectual property for Special Commercial Court judges. The activity is designed to familiarize the participants on the rules and procedures, and substantive law and jurisprudence on intellectual property thereby enhancing the capacity of judges on the efficient, effective, and expeditious disposition of intellectual property cases. BSA particularly welcomes the cooperation with the US government, noting that a number of programs last year were conducted jointly with the US Embassy in Manila and the US Patent and Trademark Office, which provided judges from both countries the opportunity to exchange experiences and discuss best practices.

Recommendation: Despite positive developments, due to continuing concerns regarding the high rates of unlicensed use of software by enterprises, BSA is recommending the Philippines as a **Country of Concern**.

ROMANIA

Although good cooperation with law enforcement continues, persistently high levels of unauthorized software use by enterprises and stalled efforts to ensure the use of licensed software by government agencies cause BSA to recommend Romania as a Country of Concern.

Overview/Business Environment

The commercial environment for the software sector in Romania, as in many other countries, is changing with the shift to new Internet-based means of deploying software solutions and services to customers. The use of unlicensed software by enterprises and government agencies remains a significant problem.

Copyright

According to the most recent data, the rate of unlicensed software use in Romania was 62 percent in 2013, representing a commercial value of unlicensed software of US$208 million.[1]

Government Legalization: BSA welcomes the increasing collaboration between law enforcement and industry groups to raise awareness of the importance of using licensed software. BSA, however, is increasingly concerned that efforts by the central government to ensure that government agencies use only licensed software have not progressed. Despite attempts by BSA members to engage with the authorities, the Romanian Government has not taken steps to ensure that all government agencies are using licensed software in accordance with the license terms and conditions.

Statutory and Regulatory Provisions: On February 1, 2014, amendments to the new intellectual property law entered into force as result of the new Criminal Procedure Code. The amendments had the effect of decreasing the penalties for most of the copyright crimes.

The new Criminal Procedure Code also provides that only certified specialists may inspect computers during investigations of suspected unlicensed software use. As a result, the economic police officers who previously conducted these inspections are no longer allowed to do so. Instead, the inspections must be performed exclusively by the organized crime units of the police, which has certified specialists, or by the Romanian Copyright Office (ORDA), which has only nine inspectors. This change in procedure is significantly impeding enforcement efforts, as the number of organized crime officers available for such inspections is considerably lower than the current number of police officers able to conduct them.

An amendment to the Criminal Procedure Code has been proposed which would allow police officers to conduct inspections, but it is unclear if this will be adopted. In the meantime, police departments should support the certification of economic police officers as specialists within the meaning of the Criminal Procedure Code. This would benefit not only intellectual property enforcement, but also enforcement of other types of crime where collective evidence requires the search of computers, such as tax evasion.

[1]Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Amendments to the Copyright Law are also being considered. BSA expects these amendments to resolve the issue of computer search warrants, the source of a long-standing problem for BSA when attempting to conduct inspections regarding unlicensed use of software by enterprises. The draft should also correct the detrimental allocation of competence of copyright crimes to the Courts of First Instance. Prior to 2010, the competence for prosecuting and trying intellectual property crimes resided with 42 tribunal courts and associated prosecutors' offices, where trained prosecutors and judges and prosecutors could focus on software infringement and other such cases. In 2010, this competence was shift to as many as 188 generalist courts and prosecutors' offices throughout the country. This has made the judicial process more challenging and has all but eliminated the possibility of focusing training resources on specialist prosecutors. Unfortunately, the proposed amendments have been pending for more than two years.

Compliance and Enforcement: In 2014, Romanian law enforcement conducted 102 inspections of enterprise end-users and 21 Channel raids in which unlicensed BSA member software was found. There were eight convictions reported by BSA members in 2014. This number of convictions is double the 2013 figure, but still very far from the 30 a year that was typical prior to 2010, when the authority for prosecuting and judging intellectual property crimes shifted from tribunals to the courts of first instance.

While authorities were active in partnering with BSA on prevention campaigns, enforcement actions have declined over the last year. Formal written instructions from the government may be needed to clarify to enforcement officials that the investigation and prosecution of software infringement remains a priority.

Technical Assistance and Education: BSA and the police have partnered in national campaigns for enterprises, raising awareness of the legal and security risks resulting from the use of unlicensed software. More than 800 such businesses have participated in local events where they receive additional information on the risks of using unlicensed software and have the opportunity of discussing such risks with BSA and police representatives.

BSA also works closely with the ORDA to promote the use of licensed software among public authorities and publicly financed entities. In addition to the legal risks, this campaign emphasizes the security and other risks associated with using unlicensed software.

In June 2014, the Supreme Council of Magistrates, with the support of the US Embassy, organized the annual cybercrime conference in Targu Jiu for a mixed audience of police officers, intelligence services, prosecutors and judges. BSA delivered a presentation explaining the many risks related to using unlicensed software, and shared a methodology guide jointly created with the police and the General Public Prosecutor's Office in 2011.

Recommendation: While good cooperation with law enforcement continues, persistently high levels of unauthorized software use by enterprises and stalled efforts to ensure the use of licensed software by government agencies cause BSA to recommend Romania as a **Country of Concern**.

SAUDI ARABIA

A lack of resources for enforcement authorities has created an environment conducive to high levels of unlicensed software use; BSA is therefore highlighting Saudi Arabia as a Country of Concern.

Overview/Business Environment

The Kingdom of Saudi Arabia (KSA) remains a market of unrealized potential due to high rates of unlicensed software use by enterprises. This can be attributed to insufficient KSA government resource allocation and non-deterrent judgments against intellectual property infringers. After a number of years of effort with limited results, last year was even more disappointing with regard to enforcement and coordination efforts.

Copyright

The most significant challenge for BSA members in Saudi Arabia is the unlicensed use of software, which has remained stagnant at roughly 50 percent for the last six years. This represents a commercial value of unlicensed software of US$421 million.[1]

Enterprise Licensing/Legalization: The use of unlicensed software by enterprises continues to be the main threat to the software sector in Saudi Arabia. Because the Ministry of Culture and Information's (MOCI) Department of Copyright is severely understaffed, it is capable of performing fewer than 30 corporate customer engagements per month in a country that has over 700,000 registered entities with the Ministry of Commerce.

Government Licensing/Legalization: The Department of Copyright has committed to upgrade and legalize the use of software by KSA government agencies, undertaking an inventory and reporting out to industry. The inventory and reporting, however, has not yet occurred. The reality is that very few accounts have actually legalized, and the bulk of ministries still will not respond to requests to discuss the matter. BSA understands that the King previously issued a decree directing all KSA government entities to use legal software, but the Ministry of Finance's (MOF) refusal to grant adequate budgets has been cited as a reason for the lack of progress. The Saudi leadership should once again issue a mandate to KSA government ministries, requiring them to procure and use only licensed software, and granting authority to MOCI to audit and enforce compliance. The government should also issue decrees directed at MOF to ensure proper budgeting for the same. The KSA government should publicize quarterly reports detailing progress in this initiative. BSA members have offered support for third-party software asset management to identify current deficiencies in government legalization and on-going mechanisms to ensure continued compliance.

Compliance and Enforcement: MOCI, the entity responsible for administrative enforcement of copyright, lacks the proper resources. With only 12-15 inspectors for a country that has several thousand resellers and over 700,000 commercial entities, MOCI is overextended and has very limited resources for

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

this huge market. Unfortunately, in the rare instance that an enforcement action is brought by MOCI, the fines imposed are far too low to serve as a deterrent. BSA urges KSA to follow through on a proposal by the previous Minister of Culture & Information to increase the number of employees by 300 (including 150 new inspectors) and to put in place appropriate incentives.

One positive enforcement development involves the Violation Review Committee (VRC), which has improved its execution dramatically over the past year. Unfortunately, the judgments issued by the VRC are insufficient to provide a deterrent. Another reason is the bottleneck at the Board of Grievances (BOG). Cases handled by the VRC are invariably appealed to the BOG (the infringer has 60 days to appeal a judgment by the VRC), and cases appealed to the BOG can take years to complete.

Neither civil nor criminal avenues offer a practical route to enforcement. Penalties are low, *ex parte* measures are unavailable, and only one prosecutor is assigned to copyright crimes.

Recommendation: A lack of resources for enforcement authorities has created an environment conducive to high levels of unlicensed software use; BSA is therefore highlighting Saudi Arabia as a **Country of Concern**.

SPAIN

Despite positive developments, continuing concerns regarding the unlicensed use of software by enterprises in the country lead BSA to recommend Spain as a Country of Concern.

Overview/Business Environment

The unlicensed or under-licensed use of software by enterprises and the availability of unlicensed software on the Internet continue to be the main challenges for the software industry in Spain. This is substantially the same as the previous year, although legislative changes, some enacted, some still pending, may help to improve the business environment.

Copyright and Enforcement

Enterprises of all types, both private and state-owned, and especially small- to medium-sized enterprises (SME's) continue to use unlicensed or under-licensed software at rates significantly higher than those observed in similar markets in Europe. According to the most recent data, the use of unlicensed software in Spain increased from 44 percent in 2011 to 45 percent in 2010, representing a commercial value of over of US$1 billion.[1]

Enterprise Licensing/Legalization: Enterprises have been slow to adopt internal controls on software in use by their organizations, contributing to high rates of unlicensed use. This lack of internal control is expected to be addressed with the approval of the new Criminal Code, making intellectual property crimes (including the willful use of unlicensed software) one of the offenses that triggers the corporate criminal responsibility (CCR) response. This will make both companies and their managers criminally liable for the unlicensed copying of business software within information and communication technology (ICT) systems of enterprises.

Statutory and Regulatory Provisions: In 2014, Spain enacted a set of reforms to the Intellectual Property Law and the Civil Procedure Law. The revision of the Criminal Code (see above) remains pending, with expectations that these amendments will be adopted in the first half of 2015.

Revisions to the Intellectual Property Law (Law 21/2014) were adopted and published on November 5, 2014 ("2014 amendments") and went into force on January 1, 2015. Article 138 of the new law establishes indirect liability for copyright infringement for (a) those who willingly induce others to infringe; (b) those who cooperate with the infringement, having knowledge of the infringement or having reasonable means to know about the infringement; and (c) those with the ability to control the activity of the infringer and with direct economic interest in results of such infringement. The indirect liability applied to these categories remain subject to the limitations on liability set forth in the Law on Information Society Services and Electronic Commerce (LSSI).

The new law also increases the powers of the Intellectual Property Commission of the Ministry of Culture to carry out action against online infringers. For example, Article 158*ter* describes the requirements with which a notice must comply in order to generate "effective knowledge" for Internet Service Providers (ISPs) without the need for formal authorization from a court of law or other authority.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Finally, changes have been introduced to Article 256 of the Civil Procedural Law, governing civil procedures to enforce intellectual property rights, enabling copyright holders to obtain an order from a civil court the identity of infringers, as preliminary evidence, prior to the formal initiation of a civil suit. There is also subject to certain limitations.

Draft amendments to the Criminal Code that were presented for parliamentary consideration in September 2013 would have allowed Spanish law enforcement to take criminal actions against enterprises that are willfully using unlicensed software. The amendments are expected to be approved in 2015. These amendments are important because instructions to prosecutors issued by the Attorney General's Office de-criminalizing infringing distributions of content by P2P networks and denying that unlicensed use of software by enterprises meet the standard for criminal prosecution. This has resulted in a cessation of criminal enforcement actions against illegal file sharing and have eliminated the possibility of prosecuting infringing enterprises.

Other shortcomings in Spain's legal framework remain. Changes are required to allow criminal and civil actions to proceed against the manufacture and sale of devices and services that are primarily designed or marketed to facilitate the circumvention of technological protection measures (TPMs) used to prevent unauthorized access to or reproduction of software in violation of the law. Spanish courts have erroneously concluded that devices primarily designed for purposes of circumvention of TPMs are lawful when capable of some ancillary non-infringing use. While these courts arguably are improperly interpreting the law, legislative amendments could clarify the intent of the law makers and ensure that the provisions function as intended to effectively prosecute the manufacture and distribution of circumvention devices. Draft amendments to the Criminal Code that would bring the definition of circumvention devices in line with the EU Copyright Directive, if adopted, could go into force by the end of 2015 and could lead to more effective interpretation by the courts.

In addition, BSA recommends further legislative amendments to the Civil Procedure Law to avoid bonds for *ex parte* inspections, to permit anonymous evidence to initiate *ex parte* inspections, and to clarify that compensation of damages must be valued at least at the full retail value of the infringed goods. Commercial Courts generally perform well, but the effectiveness of civil actions is occasionally impeded by the imposition of burdensome bonds, difficulties in obtaining the detailed evidence required to conduct *ex parte* inspections, court-imposed measures that frustrate inspections in progress, and extremely low damage awards in some cases.

Technical Assistance and Education: BSA worked with the Ministry of Industry in in 2014 to revive an important joint awareness campaign. We hope that we are able to conclude an agreement to proceed with the initiative, including an action plan with specific activities in 2015.

Recommendation: Despite positive developments, continuing concerns regarding the unlicensed use of software by enterprises in the country lead BSA to recommend Spain as a **Country of Concern**.