SPECIAL 301 SUBMISSION

February 5, 2016

Docket No. USTR-2015-0022
Christine Peterson
Director for Intellectual Property and Innovation,
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Ms. Peterson,

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 2016 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 countries based on two separate sets of criteria:

- "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, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, Salesforce, SAS Institute, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro and Workday.

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 strongly rely on the proper protection and enforcement of all forms of intellectual property and on open access to US trading partners' markets in order to continue innovating and driving the global digital economy. Adequate and effective **copyright, patent and trade secrets** protection and enforcement remains a critical element for a successful commercial environment in US trading partners for BSA members. In addition, eliminating **market access barriers** of US trading partners that discriminate against or impede BSA members in overseas markets is also critical for the continued health and growth of the software sector. Increasingly these take the form of data localization policies that restrict the ability of companies to transfer data out of the country where it is collected.

BSA members face significant challenges due to the availability and extensive unlicensed use of their software products, especially **unlicensed use of software** products or services **by governments, state-owned enterprises (SOEs), and business entities.**

In the following sections, BSA provides specific country reports on US trading partners that do not provide **fair and equitable market access** to BSA members, or fail to provide **adequate and effective protection of intellectual property**, or both. We recommend these countries be listed on USTR's Priority Watch List or Watch List. We also request that Spain be noted in the Report as a Country of Concern because of a number of ongoing enforcement issues.

Priority Watch List:	**Argentina, Chile, China, Ecuador, India, Indonesia, Russia, Ukraine, and Vietnam**
Watch List:	**Brazil, Greece, Kazakhstan, Korea, Mexico, Nigeria Romania, Thailand, and Turkey**
Country of Concern:	**Spain**

The country reports immediately following this introduction set 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 needed.

In addition to the country reports provided, we also make reference to specific concerns we have about additional countries (**Azerbaijan, Georgia, Macedonia, Panama, Poland, Taiwan , and Turkmenistan**) in this introduction and request that they be noted in the 2016 Special 301 Report.

Market Access

Cross-border data flows: Data services, including storage, processing, and analytics are the fastest growing elements of digital trade. The way in which software is used and delivered is changing rapidly. Whereas BSA members once delivered their software to consumers primarily on CD-ROMs or pre-installed on PCs, today software is more often downloaded online or used on remote servers, such as through cloud computing services. The transformation to data services and digital delivery model provides tremendous benefits to users and the ability to move data across borders is critical to both the business offerings and core operations of enterprises that make up the digital economy. Unfortunately, a number of countries, including **Brazil, China, India, Indonesia, Nigeria, Russia, and Vietnam**, have adopted or proposed rules that prohibit or

significantly restrict companies' ability to provide data services from outside their national territory.

Data market access barriers requirements take many forms. Sometimes they expressly require data to stay in-country or impose unreasonable conditions in order to send it abroad; in other cases, they require the use of domestic data centers or other equipment. Sometimes they are justified as necessary to protect privacy, security or to obtain jurisdiction over these services. But too often, there is also an element of protectionism, as the means chosen by these governments tend to be significantly more trade-restrictive than necessary to achieve any legitimate public policy goal.

Recognizing the trade disruptive impact of measures that impede cross-border data flows and mandate data localization, the United States insisted and succeeded in including specific prohibitions against such practices in the recently concluded Trans-Pacific Partnership Agreement (TPP).[2] BSA strongly supports this important outcome and urges the United States Government to seek similar results through all available trade mechanisms, including Special 301.

Procurement Discrimination: Governments are among the biggest consumers of software 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 software products and services include **Brazil, China, Ecuador, India, Indonesia, Nigeria, Russia, Taiwan, and Vietnam.**

Security: Governments have a legitimate interest in ensuring that software products and services and the equipment 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, Nigeria, Russia, the United Kingdom, and Vietnam**.

Standards: Technology standards play a vital role in facilitating global trade in information technologies (IT). 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 of 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 IT products include **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

[2] TPP Agreement – Articles 14.11 and 14.13 available at https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text

difficult. For example, **India** has recently suspended Guidelines on patentability of software-enabled inventions.

Some countries have adopted or are considering policies that could significantly constrain the freedom of patent holders to 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. In **South Korea**, a similar policy has recently been approved. **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 and other Proprietary Information: 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 **Brazil, China, Indonesia, and Nigeria.**

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.[3] Not only does unlicensed use of software impact the revenue stream of BSA members, deterring investments in further innovation, but the use of unlicensed software also exposes enterprises and agencies engaged in such activity to higher risks of malware infections and other security vulnerabilities.[4]

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 countries. **Mexico** has been a leader in this regard.

[3] 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.

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

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 to enable BSA members to 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 or of the inability or unwillingness of authorities to enforce the law. In addition to the countries explicitly cited in this submission, examples of countries where enforcement against enterprises that use unlicensed software in the course of their commercial activities is inadequate include **Azerbaijan, Georgia, and Turkmenistan.**

The judiciary also has an important role to play to ensure rights owners have access to proper remedies against intellectual property infringement. For example, triple damages were available for copyright infringement under **Poland**'s copyright law but, in late June 2015, the Polish Constitutional Tribunal declared that the triple damages provision was unconstitutional. The Polish copyright law now lacks clarity regarding the availability of multiple damages, which will likely hamper enforcement efforts in country.

Government and SOE Legalization: The use of unlicensed software by governments 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 do on our own. BSA applauds the inclusion of a specific provision mandating the exclusive use of legal software by governments in the recently concluded TPP Agreement.[5] We urge the United States Government to use all available trade mechanisms, including Special 301, to aggressively engage with US trading partners on behalf of US companies on this important issue.

Some governments, like **Mexico**, have taken commendable 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)[6] some government agencies in **South Korea** continue to under-license the software they use. Similarly, efforts have been made to address software that is under-licensed by government agencies in **Panama**. No progress has been made to date, despite commitments in the US-Panama Trade Promotion Agreement. **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 **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.

[5] TPP Agreement – Article 18.80(2), available at https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text
[6] 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.

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. The use of unlicensed software by government agencies has been increasing in Taiwan over the past few years. Even when Taiwanese agencies recognize the use of unlicensed software, they may not take the necessary steps to address the issue. Furthermore, procurement practices in **Taiwan**, often request or require that hardware be offered without preinstalled operating systems and other software. It is critical for **Taiwan** to establish clear oversight to ensure that software subsequently installed is fully compliant with relevant software licenses and that agencies are prohibited from installing or using unlicensed software on such machines.

The high levels of use of unlicensed or under-licensed software by government agencies in **Macedonia** is also a great concern.

Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the 2016 Special 301 Report and the US Government's engagement with important trading partners in 2016. 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

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 2015 it deteriorated as a result of monetary policies and an overall declining economic environment. There was very little political will to elevate the importance of the protection and enforcement of intellectual property during former President Kirchner's tenure, and law enforcement authorities did not consider intellectual property infringements a priority.

It is important to note that during his presidential campaign, President Mauricio Macri, who took office on December 10 2015, pledged to open the currency exchange market and to review Argentina's income tax regulations; both policy changes have the potential to benefit the overall business environment in the country. The business community hopes President Macri will be more inclined than his predecessor to engage in a dialogue with the private sector on the need to implement reforms to better protect intellectual property in Argentina.

Market Access

Due to broader economic circumstances, the Kirchner government imposed severe currency exchange restrictions, prohibiting the payment of dividends and royalties to foreign parties. This, in turn, made 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. President Macri has committed to working on this issue but it is still too early to determine what, if any, changes to the Kirchner currency policies will be made.

BSA has previously noted that 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; as a result, a corporation 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. President Macri has pledged to implement income tax reforms and this may present an opportunity to implement the necessary changes to address the issue. There is also a clear need for the United States and Argentina to reach an agreement on a treaty to avoid double taxation. The difficulty to obtain foreign currency, however, has superseded these tax issues.

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.

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 guidelines have been issued by 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 persons 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 59 cases in 2015 and it has approximately 30 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.

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**.

[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.

CHILE

Due to ongoing 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 Chile remain on the Priority Watch List.

Overview/Business Environment

The overall business environment for software in Chile remained largely unchanged in 2015. According to the most recent data, the rate of unlicensed software in 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 Nueva Mayoría Government has not issued or changed any policy to specifically address unlicensed use of software. Inadequacies in the law remain unaddressed and remedies for unlicensed software use are 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 technology 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 some progress on government software legalization in Chile, further steps are necessary. Chile is a Party to the Trans-Pacific Partnership (TPP) and the agreement establishes that Parties must ensure that their central government agencies use only licensed software[3]. Chile should implement changes to its domestic regulations to comply not only with its US-Chile FTA commitments but also with TPP.

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

[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

[3] Trans-Pacific Partnership Agreement Article 18.80.2

verifiable software asset management procedures, during which 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 licensed users are able to access their software products and services.[4] 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. TPP also requires measures that prevent circumvention of technological protection measures[5].

Compliance and Enforcement: BSA enjoys a good relationship with the Chilean intellectual property agency, INAPI. During 2015, BSA conducted almost 70 civil compliance inspections of a variety of enterprises on behalf of our members.

In order to conduct civil inspections, civil *ex parte* actions remain a critical remedy for 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.[6]

Recommendation: Due to ongoing 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 Chile remain on the **Priority Watch List**.

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

[5] Trans-Pacific Partnership Agreement Article 18.68

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

CHINA

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

Overview/Business Environment

The commercial environment in China for software and information technology has become more challenging during 2015. For many years, BSA members have struggled with 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 rationalized as a combination of cost-savings measures and as efforts to promote the domestic software industry.

In 2015, the Government of China continued to issue security related policies that effectively act as procurement preferences and other market access barriers. These include sweeping security-related legislation as well as sector-specific cybersecurity regulations for the banking and insurance sectors which request or require firms in these sectors to replace existing systems with "secure and controllable" products and services. BSA members are very concerned that these policies could effectively block them and other US suppliers from an increasing number of important sectors in the Chinese economy.

China's existing regulatory regime also makes it extremely difficult for BSA members to invest in the digital market. There has been very limited progress in reforming the existing system, which effectively excludes foreign investment especially in cloud or other data-services in China. Except for a conditional and limited opening in the electronic commerce field, China continues to regulate Internet Services as Value-Added Telecommunications Services (VATS) and precludes granting licenses to wholly-owned or majority-owned foreign entities.

These policies, combined with broader "indigenous innovation" policies, contribute to an increasingly challenging 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 (IP) environment also remains extremely challenging. BSA is monitoring developments related to patent law reform, copyright reform, proposals to regulate the reward and remuneration of employee-inventors, and policy and legal developments regarding competition policy and the utilization of patents and other IP. We also urge 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. The level of legal software per PC in China remains well below the level in other markets, including emerging markets at comparable levels of economic development with China, indicating continuing high rates of unlicensed software use. 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 (SAM) procedures. Such procedures would include government agencies having audits conducted of the software they have installed to ensure not only that all copies in use are properly licensed, but also that the organizations are using relevant software efficiently and cost-effectively, and to reduce cybersecurity threats associated with using unlicensed software.

While there is some hope that ongoing IP-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 companies. Such engagement should continue via ongoing 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) negotiations, and negotiations over 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 technology market. While ensuring the security of government systems and important economic sectors is appropriately 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 IT products and services should not be limited to those with IP that is locally owned or developed, nor should it depend on the transfer of IP to Chinese domestic firms. Incentives for encouraging investment in research and development (R&D) facilities in China should not include requirements for doing so in order to provide products and services to the market.

Security: In December 2015, China passed the Counter-Terrorism Law. An earlier draft of the law raised many concerns including requirements to "pre-install technical interfaces", "submit cryptographic solutions", and "place related equipment and store domestic related data within China." Although these requirements are not present in the final law, concerns remain regarding other provisions that impose vague and/or burdensome requirements on companies that may not be the most efficient way to curb terrorism. For example, telecommunication business operators and Internet service providers are generally obliged to "provide technical support and assistance, such as technical access and decryption" to law enforcement agencies and appear to be required to monitor content for extremist communication.

In July 2015, the National Peoples' Congress (NPC) released a draft Cybersecurity Law that would create a firmer legal basis for the activities of the Cybersecurity Administration of China, impose a variety of obligations on "network providers", impose additional security and testing requirements and security "reviews" on certain software and IT products and services, limit data flows, and establish a prescriptive personal data protection regime. BSA urges the Government of China to adopt an effective cybersecurity strategy that enhances the cybersecurity capabilities of enterprises and other institutions that is consistent with international standards and approaches, does not impose unnecessary administrative compliance burdens, and does not discriminate against BSA members.

In addition to legislative developments, there have been a number of security-related regulatory developments that raise significant market access concerns. In late 2014, the China Banking Regulatory Commission (CBRC) issued Circular No. 39 (Guiding Principles on Strengthening the Banking Network Security and Information Technology Infrastructure through Secure and Controllable IT) and Circular No. 317 (Guidelines on Promoting the Application of Secure and Controllable IT, Year 2014-2015) which require that "by 2019, 75% of information technology employed by the financial sector should be 'secure and controllable.'" The regulations included concerning provisions including source code disclosure mandates, requirements to use indigenous IP, and obligations to share encryption solutions, among others. Fortunately, after concerns from many stakeholders were raised, the CBRC rescinded the guidelines and is reportedly working on a new approach. BSA encourages the Government of China to adopt a cybersecurity strategy for China's financial sector that is effective, consistent with international practice, and does not impose unnecessary burdensome requirements.

In a related development, in October 2015 the China Insurance Regulatory Commission (CIRC) issued the draft "Supervision Rules on Insurance Institutions Adopting Digitalized Operations." While not as prescriptive as the initially issued CBRC rules, the draft measure still raised significant concerns with BSA and our members. To some extent, the draft Rules presuppose far more capability and interest in non-specialized technology firms in installing and managing their own software and systems. We also identified concerns such as apparent requirements to use domestic standards, even if international standards already exist, data localization requirements, third party auditing requirements, general prohibitions on "outsourcing", and other elements. Many such provisions appear designed to limit, or would at least have the effect of limiting, foreign software and technology companies from offering products and services to China's insurance sector.

In addition to emerging policies, BSA continues to urge reform of long-standing measures, such as the Multi-Level Protection Scheme (MLPS). The MLPS imposes significant restrictions on procurement of software and other information security products for an overly broad range of information systems the government considers sensitive. Among other requirements, procurements of such products are limited to those with intellectual property rights owned in China. This applies to procurements by the 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. Furthermore, there appear to be explicit references to the MLPS in the recently enacted National Security Law and the draft Cybersecurity Law (see above).

BSA welcomed China's commitment during the 2012 JCCT that it will review and revise the MLPS while seeking the views of all parties, including US parties. BSA urges China to use this process to remove requirements that discriminate against foreign-supplied products and services, or those products and services that have foreign-owned intellectual property.

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 (Catalogue). In December 2015, MITT issued the final Catalogue, which is expected to go into force on March 1, 2016. The revised Catalogue continues to treat cloud computing and other Internet-based services as VATS; this designation carries significant restrictions on foreign investments. This treatment of cloud computing as a VATS is not in keeping with the general practice of other markets.

Encryption: China maintains its 1999 Commercial Encryption 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 to foreign products, particularly if authorities begin applying the regulations more broadly. The regulations also run 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.

Procurement: BSA remains significantly 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...."

BSA urges the Chinese Government to withdraw the discriminatory elements in government procurement policies, including price controls and site-license preferences, and to 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; 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.

Intellectual Property

Intellectual Property and Competition: The State Administration of Industry and Commerce (SAIC), one of three Chinese agencies responsible for Anti-Monopoly Law (AML) enforcement, published the "Rules

of the Administration for Industry and Commerce on the Prohibition of Abuses of Intellectual Property Rights for the Purposes of Eliminating or Restricting Competition" (SAIC IPR Abuse Rules) in early 2015. These Rules provide internal guidance for the SAIC when conducting AML enforcement investigations involving IPR. They do not, however, bind other AML enforcement agencies. Despite various rounds of comments by BSA and others, the SAIC rules still 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. Later in 2015, the National Development and Reform Commission (NDRC) and SAIC both started working on their respective versions of IPR Abuse Guidelines. The State Council Anti-Monopoly Commission (AMC) will presumably eventually issue one final set of Guidelines that will bind all three AML enforcement agencies. However, to the extent that the Draft Guidelines differ between the different agencies and the existing SAIC IPR Abuse Rule, the situation creates many uncertainties for BSA members and other entities in China, both global and domestic. The US government should continue to urge China to avoid using AML enforcement to undermine or prevent the normal and legitimate exercise of IPR.

Patent Enforcement: The State Intellectual Property Office (SIPO) is leading efforts to amend the Patent Law. Among other things, the proposed amendments would expand the enforcement powers of SIPO and its subsidiary agencies at the provincial and local levels of government. These agencies would then be able to conduct *ex officio* raids and enforcement actions against ill-defined "market-disruptive" patent infringement activities, and award fines and other penalties. This creates enormous risks for 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.

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) 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 an overly broad view of the term "invention." 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.

Although the draft regulations have been pending several years, it appears that SIPO is reviving efforts to move forward with regulations on service inventions. 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.

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 in 2013, 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 (SAM) best practices; (c) sufficient budgets to properly procure licensed 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 procurement of domestic software brands as part of the legalization process.

Statutory and Regulatory Provisions: The third draft of amendments to the Copyright Act remains under review by the State Council Legislative Affairs Office (SC/LAO). There is an urgent need for China to update and modernize its Copyright Law. BSA urges the Government of China 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 in the cloud;
- Increases statutory damages, at least so that they are in line with the revised Trademark Law and ongoing amendment of the Patent Law;
- Ensures that protections for technological protection measures (TPMs) extend to access controls, that the unauthorized sale of passwords and activation codes are explicitly defined as TPM circumvention, and that constructive knowledge circumvention is sufficient to demonstrate a violation of the law; and
- Strengthens procedural provisions, for example to explicitly grant courts more authority to compel evidence preservation and grant preliminary injunctions.

BSA is disappointed that recent amendments to China's Criminal Code do not address the widespread use of unlicensed software by enterprises in China. The Government of China has not made the necessary changes to the IPR-related provisions of the Criminal Code (e.g., Articles 217 and 218 and accompanying judicial interpretations (JIs)) and other related provisions. This represents an important missed opportunity to apply appropriate criminal remedies to copyright infringements which undermine 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.

market and the incentives to bring to, or develop in, China cutting edge software solutions. BSA continues to urge the Government of China to reconsider the decision not to amend IPR-related provisions. China should impose criminal liability on enterprises that use of unlicensed software, consistent with international best practices. BSA urges that the following issues be addressed and improved:

- Reduce thresholds that are too high (e.g. 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 not clear, law enforcement authorities have been reluctant to impose criminal liability on commercial enterprises using unlicensed software in the course of their business operations; and
- Define, distinct from copyright infringement, criminal violations for unauthorized circumvention of TPMs and trafficking in circumvention technologies, software, devices, components, and services, including in particular the unauthorized sale of passwords or product activation codes or keys.

In addition to correcting the scope of criminal liability for IP violations, the Government of China should also amend the Criminal Code 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, like Beijing and Jiangsu.

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 must increase the amount of damages awarded against enterprises found using unlicensed software. While some courts have increased damage awards, 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 draft 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 (IP Courts) in Beijing, Shanghai, and Guangzhou. The IP 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, the IP Courts have jurisdiction over patent cases and software related copyright cases. Establishing the IP Courts demonstrates the Government of China's growing interest in building more effective judicial enforcement mechanisms for the protection of IP. BSA and its members have had some success with the IP Courts, although we are observing capacity issues as the limited resources of the three new IP Courts are tested against the growing backlog of cases. BSA is looking forward to continued improvements in the efficiency and quality of judicial decisions from the IP 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. 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 a deteriorating market access environment for the software and information technology (IT) sectors and continuing high levels of unlicensed software use by enterprises, BSA recommends that China be maintained on the **Priority Watch List**.

ECUADOR

Due to Ecuador's failure to rescind decriminalization of intellectual property infringement, persistently high levels of unlicensed software use, and the significant tariff and non-tariff barriers to technology products and services, BSA recommends that Ecuador remain on the Priority Watch List.

Overview/Business Environment

Lax intellectual property enforcement and high tariff and non-tariff barriers make Ecuador a difficult place to do business. In the wake of the complete decriminalization of intellectual property infringement in 2014, unauthorized software use in the government and private sector remains widespread. While other enforcement tools remain available, such as confiscation of infringing products and monetary penalties, they are insufficiently deployed to be effective.

In addition, recently adopted and newly proposed policies to restrict the use of cross-border cloud computing services and a proposed open-source software requirement for public entities threaten the ability of US software, Internet, and other information technology (IT) firms to provide products and services to the market. BSA urges the US government to engage Ecuador in consultations to address these obstacles and ensure that Ecuador meets its existing international commitments.

Market Access

Mobile phone quotas: As noted in USTR's NTE report for 2015, Ecuador has maintained strict quotas on mobile phone imports since 2012.[1] These measures reduce Ecuadorians' access to cutting edge technologies as well as productivity-enhancing software and services delivered over the Internet. In addition, the restrictions generate illegal traffic in mobile phones.

Safeguards: In March 2015, Ecuador began imposing surcharges of up to 45 percent on nearly a third of its imports, including many intellectual property-intensive IT products. Ecuador notified the World Trade Organization's (WTO) Balance of Payments Committee about these measures in April, but numerous WTO members have argued that the measures are not economically justified and may be inconsistent with WTO rules. The measures remain under review by the Balance of Payments Committee.[2]

Procurement: The National Secretary of Public Administration's Agreement No. 166, dated September 19, 2013, prohibits the federal public sector from using cloud email services hosted in servers outside Ecuador. Furthermore, the *Código Orgánico de Economía Social del Conocimiento e Innovación* ("Knowledge Code") under consideration by the National Assembly would extend the data localization requirement to all cloud computing services procured by the government. The Code would also require public sector entities to purchase only open-source software. [3] Together, these measures stand to prevent

[1] COMEX Resolution No. 67 of 11 June 2012, http://www.aduana.gob.ec/contents/nov/news_letters_view.jsp?anio=2014&codigo=83, and subsequent resolutions.

[2] WTO, "WTO Members Remain Divided on Ecuador's Import Surcharge for Balance-of-Payments Reasons, October 16, 2015. https://www.wto.org/english/news_e/news15_e/bop_16oct15_e.htm. As noted in this document, the top surcharge rate was reduced to 40 percent in January 2016.

[3] Article 136 of the draft Code: http://coesc.educacionsuperior.gob.ec/index.php/LIBRO_III:_De_la_Gesti%C3%B3n_de_los_Conocimientos.

Ecuador's government from accessing best-in-class, cloud-based ITC services, with significant costs in terms of lost efficiencies and lower productivity.

Copyright and Enforcement

Changes to Intellectual Property Laws: Ecuador's Intellectual Property Law (No. 83, enacted on May 19, 1998) included an entire chapter on crimes and punishment for intellectual property infringement, including criminal provisions relating to infringements of patents, plant varieties, well known trademarks, commercial secrets, geographic indications, and copyrights.[4] However, as noted in USTR's Special 301 Report for 2015, the Penal Code enacted by Ecuador in 2014 decriminalized any and all infringement of intellectual property (IP). These measures appear to be inconsistent with Ecuador's commitments under the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), notably Article 61, which requires member states to provide minimum criminal protection in cases of willful trademark counterfeiting or copyright infringement on a commercial scale. They are also inconsistent with Ecuador's trade agreement with the European Union, under which the parties reaffirm their rights and obligations under TRIPs.[5]

In the 2015 Special 301 Report, USTR suggested that, "If Ecuador reinstates the repealed provisions or adopts new acceptable procedures and penalties by December 30, 2015, USTR will promptly conduct an OCR to determine whether to return Ecuador to the Watch List." This timetable was not met.

Enforcement: Ecuador's Intellectual Property Law enables the National Directorate of Industrial Property at the Ecuadorian Intellectual Property Institute (IEPI) to take administrative actions to counter IP infringement. In cases where IEPI determines IP has been infringed, the agency may confiscate infringing materials and assess monetary penalties. However, IEPI's activity on enforcement is low, and this, combined with the repeal of all criminal penalties for infringement, has led to persistently high levels of unauthorized software use in both government and the private sector.

Enterprise Licensing/Legalization: According to BSA's Global Software Survey, 68% of Ecuador's installed software was unlicensed in 2013 (latest available data), unchanged from the previous survey in 2011. This unlicensed software has a commercial value of $130 million.[6]

Proposed ban on pre-installed software on mobile devices: The draft Knowledge Code would require electronic devices sold in Ecuador, including mobile phones and tablets, to be sold without pre-installed software, opening a pathway for widespread use of unlicensed software on these devices.

[4] Ecuador is a member of the World Intellectual Property Organization (WIPO) and is a signatory to the Paris Convention, Berne Convention, the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), the Patent Cooperation Treaty (PCT), and Andean Decision No. 486, the Common Intellectual Property Regime for the Andean Countries

[5] Article 196. Text available here: http://trade.ec.europa.eu/doclib/press/index.cfm?id=1156. The parties have completed negotiations but have not yet ratified the agreement.

[6] 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 Ecuador's failure to rescind decriminalization of intellectual property infringement, persistently high levels of unlicensed software use, and the significant tariff and non-tariff barriers to technology products and services, BSA recommends that Ecuador remain on the **Priority Watch List**.

INDIA

Although there have been recent positive developments on market access issues and intellectual property enforcement in India, BSA members still face challenges in providing products and services to the market, as well as persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends India remain on the Priority Watch List.

Overview/Business Environment

A series of government announcements by the current administration such as the establishment of the Digital India initiative, the establishment of Commercial Courts, 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 for the software industry in India. The initiatives remain in early phases of implementation. Therefore, it remains premature to assign actual improvements to the commercial environment based on these developments.

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 signs that the environment could deteriorate rather than improve. Government procurement policies remain outmoded and inefficient because of local content preferences and technology preferences such as for Open Source Software (OSS).[1] Such policies do not offer a level playing field to US 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. 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 nearly US$3 billion.[2] 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.

In October 2015, an Ordinance was enacted that brought into force the *Commercial Courts, Commercial Division and Commercial Appellate Division of High Courts Bill, 2015*. The Ordinance also clarifies that Commercial Courts have jurisdiction over intellectual property rights (IPR) and related matters and imposes limits on the time the Courts may take to decide cases. Both of these considerations are important because they may allow IPR-related cases, including those related to the unlicensed use of software, to be brought before a specialist court, and may also solve the very long case pendency problem in related civil-litigation in India. This is particularly relevant since cases that may drag on for many years

[1] http://deity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf

[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.

and undermine both the incentives to bring IPR-related cases in the first place, or to settle them in a timely fashion.

Unfortunately, enforcement against enterprises using unlicensed software remains a challenge. Due to a recent Supreme Court judgement, [3] software companies experiencing license infringement are forced to file cases across the country in District and High Courts, where the experience and knowledge to handle such cases varies and we find uneven willingness to impose preliminary injunctions and important forms of preliminary relief.

Market Access

The Government of India, at the central and state levels, has adopted a variety of policies affecting the commercial environment for BSA members and the information technology (IT) 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 IT sector investment and growth in India. Domestic preferences and technology mandates in public procurement, as well as 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 Government of India to foster a more transparent and effective policy environment that will drive investment and deployment of cutting edge technologies and services, which will in turn drive the digital economy and benefit Indian businesses, government agencies, and consumers.

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 2015. The Department of Electronics and Information Technology (DietY) has recently issued a request for proposal (RFP) for provisional accreditation of cloud service providers (CSPs) which mandates that all data and services provided by the CSPs need to be located in India. There is strong evidence that such policies are harmful to India as they reduce productivity and dampen domestic investment in the country.[4]

Similarly, the draft Machine-to-Machine (M2M) Roadmap, issued by the Department of Telecommunication (DOT) in January 2015, proposed to require all M2M gateways and servers be located in India only "in the interest of national security." BSA was grateful that the DOT listened to the views of BSA and other stakeholders[5] and removed this unnecessary and counter-productive requirement in the final M2M Roadmap issued May 12, 2015.[6]

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'

[3] Indian Supreme Court Judgement in IPRS v Sanjay Dalia & Anr.,1st July 2015

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

[5] http://ww2.bsa.org/country/News%20and%20Events/News%20Archives/hi/2015/hi-05192015-Machine-to-MachinePolicyIndia.aspx?sc_lang=hi-IN

[6] http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

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. In September 2015, India published a National Encryption Policy that was withdrawn shortly after publication. The draft raised a number of concerns including restrictions on use of commercially available encryption (by restricting key lengths for example) and mandates to disclose proprietary information. BSA urges the Government of India to carefully consider the implications of a potential encryption policy and to promote an ample dialogue with all stakeholders before any decisions are made.

Privacy: BSA members increasingly offer data services to their customers. BSA members invest in significant efforts to ensure that the sensitive information of their customers is used appropriately and fully protected. 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 is still being discussed by the relevant government departments. BSA encourages the Government of India to seek public comments on the draft bill and 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.

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 scholars, and others. On December 19, 2014, the first draft of the National IPR Policy was issued by the IPR Think Tank.

In early 2014, BSA filed written comments to the IPR Think Tank on the draft National IP Policy. 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.

BSA understands that the IPR Think Tank submitted its final draft to the DIPP at the end of 2015. Neither the Think Tank, nor DIPP have formally requested public comments on that draft. The draft includes a number of initiatives targeted at strengthening existing IPR laws and IPR-related administrative and procedural mechanisms. The draft also recommends improving the judicial infrastructure. However, the draft does not consider amendments to provide for statutory damages in intellectual property-related matters. The final National IP Policy is expected to be published by DIPP in 2016.

Given the importance of the National IP Policy in guiding IPR-related administrative and legislative developments, and the importance of such IPR reform to enhancing India's efforts to promote an innovation based economy, we urge DIPP to conduct an open and transparent process to solicit input from all interested stakeholders before finalizing the policy.

Patentability Guidelines for Computer Related Inventions: The Office of the Controller General of Patents, Designs, and Trade Marks issued Revised Guidelines for Examination of Computer Related Inventions (CRIs) ('Guidelines') on August 21, 2015. The Guidelines were an improvement over earlier versions and appeared to allow software-enabled inventions to be eligible for patent protection. Unfortunately, in late 2015 the Guidelines were suspended due to concerns from the civil society and other stakeholders. Patent protection is vital to the software industry and it is important that the Guidelines clarify how the Patent Act applies to computer related inventions. BSA urges the Government of India to reverse the suspension of the Guidelines and to continue to promote investment in the development of computer related inventions in India.

Patent Guidelines: The Government of India is well informed of the concerns that BSA members and other entities have expressed regarding Form 27 of the Guidelines for Search and Examination of Patent Applications (Patent Guidelines). The Form mandates that a company specify the details of the working of each and every patent granted in India on an annual basis. Recently, the DIPP proposed draft amendments to the Patent Guidelines. Instead of doing away with Form 27, DIPP's proposed changes make the Form more ambiguous and compliance more difficult. The information requested, especially for high-technology industries such as the software industry, is often difficult if not impossible to provide. The requirements of Form 27 serve as a disincentive to innovators considering to seek patent protection for their inventions in India. BSA recommends that the Government of India remove Form 27 from the patent system.

Compliance and Enforcement: The lack of statutory damages and inadequate damage awards in civil enforcement continues to be a challenge for BSA and our members when attempting to enforce our rights against enterprises using unlicensed software in India. The willingness of Indian courts to grant preliminary or interim injunctions varies, and the system suffers from significant procedural delays.

The software sector has maintained good engagement and positive relationships with India's IPR enforcement authorities. Criminal enforcement, however, has not proved 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 priority of enforcement authorities to address other major crimes. This makes establishing an effective civil enforcement system all the more important.

Technical Assistance and Education: BSA is actively engaged with the government of India on a variety of matters affecting the software industry in India. The following are examples of BSA engagement with various government agencies, including at the state and local level.

- BSA, in partnership with MAIT (the Manufacturers' Association for Information Technology) and Accenture, organized workshops on Good Procurement Practices for Information Technology for government procurement officials in the states of Telengana, Kerala, Pondicherry, Assam, Punjab, Haryana, and Manipur.
- BSA, in partnership with Confederation of Indian Industries (CII), organized a one-day Conference on Intellectual Property Rights (in Technology) Adjudication under the aegis of High Court of Judicature at Madras and Tamil Nadu State Judicial Academy.

Recommendation: Although there have been recent positive developments on market access issues and intellectual property enforcement in India, BSA members still face challenges in providing products and services to the market, as well as persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends India remain on the **Priority Watch List**.

INDONESIA

Due to a worsening market access environment for the software and information technology (IT) 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 software and information technology (IT) 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 enactment of the new Copyright Law No. 28/2014 was a positive development, 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 effectively deter future infringements.

Market Access

A variety of policies affecting the IT 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 and Cross Border Data Flows: The Ministry of Communications and Information Technology (MCIT) is in the process of developing implementing regulations for Government Regulation No. 82 on the Implementation of Electronic Transactions and Systems (GR 82), which was issued in 2012. There is still considerable uncertainty regarding certain key concepts in GR 82 and the scope and implementation of the regulations.

MCIT released the draft Regulation on Protection of Personal Data in Electronic Systems in July 2015 ("Draft Electronic Data Protection Regulation"). BSA is concerned about a number of aspects regarding this draft regulation. These include local data center mandates for public services, requirements to obtain written consent to provide a wide range of data operations, and requirements that all systems used for data treatment be "certified." Such requirements will increase costs and harm the quality of data services and interfere with ensuring data security without enhancing personal information protection. BSA has submitted comments urging the Government of Indonesia to take an approach to privacy that is consistent with international practice, and that facilitates responsible and accountable utilization of personal information while allowing for cross-border data transfers.

In addition, in October 2015, the government initiated a draft bill on the Protection of Private Data ("Draft Privacy Law"), which is currently being discussed by the House of Representatives. Should it pass, the bill would represent Indonesia's first overarching law on data privacy. Thus far, however, the

government has not consulted the public on the Draft Privacy Law. It is also presently unclear how it would interact with the Draft Electronic Data Protection Regulation.

In addressing the issue of data protection in Indonesia, we encourage the Indonesian government to carefully consider the comments and recommendations BSA has submitted in the context of the Draft Electronic Data Protection Regulation, to seek public comments on the Draft Privacy Law, and to ensure that there is close alignment between the two aforementioned pieces of legislation before finalizing them. BSA also urges Indonesia 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.

Local Content and Local Manufacturing Requirements: In 2015, MCIT issued the Ministerial Decree on Local Content for LTE Technology, which imposes onerous local content requirements on a wide range of technology devices and products. The Ministerial Decree was signed jointly by MCIT and the Ministries of Trade and Industry in early July 2015 and is expected to be strictly enforced by January 2017. The rules require that all covered products would need to contain 30-40 percent (depending on the particular product) local content in order to be sold in Indonesia. The Ministry of Industry confirmed in July 2015 that local content includes both hardware and software[1].

Closely related to the issue of Local Content, in 2013, the Ministry of Trade has also passed regulations requiring importers of certain IT products including smartphones, laptops, and tablets to put in place local manufacturing facilities within 3 years from the date of obtaining their import license. If strictly enforced, this will effectively prevent the import of foreign-made IT products into Indonesia.

The stated purpose of these policies is to encourage local manufacturing and industry development. However, by blocking foreign companies without local production or development facilities from the Indonesian market, and requiring companies who wish to support the market to structure their global supply chains, these policies will effectively reduce the supply of innovative technology devices and products in Indonesia, and also hinder local companies from learning and developing the necessary experience to compete in the global arena. This will harm Indonesia's broader economic development objectives in the long run. We believe that Indonesia can better achieve its economic objectives through regulatory policies that incentivize the development of knowledge-based industries, such as software and application development, rather than through the adoption of market access barriers such as local content and local manufacturing requirements.

Source Code Disclosure Requirement: The Indonesian government released a draft Regulation on Electronic Systems Software in July 2015. If implemented as drafted, the regulation would require electronic system providers responsible for managing or operating computer systems used in connection with public services to disclose software source code. BSA is deeply concerned about this requirement. Many global companies of leading-edge security technologies will withdraw from bidding opportunities that would require them to turn over or make available their intellectual property, such as source code and other design information, limiting the choices of products and services available to public services. BSA

[1] The Ministry of Industry is still formulating the methodology for calculating the local content percentage. While the methodology will allow for software (e.g. apps) to count towards (and even comprise the entire) local content percentage, this will only be for software that is locally produced and run out of local data centers. It will not be possible, for example, to take into account the overall economic contributions that foreign software corporations make to the Indonesian economy (e.g. software donations or other investments).

strongly urges the government of Indonesia to eliminate the requirement. As of the January 2016, the regulation was still pending.

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.[2]

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 are considered infringement. Importantly, the law now provides prohibitions against the circumvention of technological protection measures (TPMs), including both access controls and copy controls. Clear provisions prohibiting trafficking in devices, technologies, and services primarily designed to circumvent TPMs are still needed. In addition, the new copyright law doubles criminal penalties for copyright infringement. Effective implementation of the law will be key to improve intellectual property protection in the country.

Compliance and Enforcement: There was little improvement in enforcement in 2015. Police will support conducting enforcement actions 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.

Judges in Indonesia often award only very low damages and legal expenses are not recoverable so the plaintiff has to bear the costs of bringing proceedings. Therefore, rights holders tend to initiate very few civil copyright infringement cases.

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.

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

[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.

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 ongoing 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 technology firms to provide products and services to the market. The US government should engage in consultations with the Russian government to urge Russia 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: On September 1, 2015, Federal law No. 242-FZ dated July 21, 2014 came into force. The Law obliges personal data processors to store personal data of Russian citizens in databases 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 the data collection. In case of non-compliance, the Law empowers Roscomnadzor to block access to the unlawfully collected personal data and establishes a detailed procedure for blockage of the website or web page containing such personal data. This is one of the most restrictive data localization laws in the world. As such, it will severely negatively impact both foreign and domestic companies. The European Center for International Political Economy has estimated this law may potentially cost the country 0.27% of its GDP.[1]

Procurement: Federal Law No. 188, dated June 29, 2015, and Regulation No. 1236, dated November 16, 2015, which are expected to enter into effect in early 2016, impose restrictions on the public procurement of foreign software. The Federal Law establishes a register of Russian software and defines the criteria for software to be considered "Russian" (copyright in the software must belong to the Russian authorities, Russian citizens, or Russian legal entities which are not controlled by foreigners; software should be legal; foreign stakeholders of a Russian software producer cannot receive more than 30% of the annual software licensing revenue of that Russian software producer). Federal and state authorities will be required to procure "Russian" software unless certain limited exceptions apply.

Other Market Access Issues: Draft Law No. 804140-6 was registered in the State Duma on May 29, 2015, and passed the first reading on October 23, 2015. The Draft Law establishes administrative liability for the search engine operator for failure to satisfy Russian citizens' claims to delete web links with

[1] The "Data Localisation in Russia: A Self-imposed Sanction" report published by The European Center for International Political Economy is available at http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/

information on him/her. A fine of up to 100,000 rubles and administrative liability for failure to fulfill court decisions on this issue may apply.

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.[2]

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. The Russian government should also develop procedures for the acquisition of licensed software from Russian and foreign software vendors by government agencies and state owned enterprises. The adoption of effective, transparent, and verifiable software asset management procedures, in which 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 enforcement actions by police has declined significantly. There was an acceleration of this troubling trend in 2015. This has been due, in large part, to a reduction in the number of police assigned to perform enforcement activities and in the number of adequately trained officers available 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 cases and they are hesitant to work on such 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 2015, 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.

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

[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 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, ongoing challenges in the administrative and judicial systems, and onerous market access barriers, BSA recommends that Russia remain on the **Priority Watch List**.

UKRAINE

Due to the lack of any concrete positive changes to protect software copyrights, the absence of a tangible plan for software legalization in the public sector, and a significant decrease in enforcement activity, BSA recommends Ukraine be placed on the Priority Watch List.

Overview/Business Environment

In 2015, geopolitical and military conflicts affected Ukraine, both of which caused significant negative impact on the country's economy. Ukraine has, however, managed to set a path for recovery based on international agreements and attention to the current account balances. Debts have been restructured and a large IMF program was approved. There are renewed expectations for reform in light of passage of the *Law on Public Procurement* and a new emphasis on rooting out corruption. It is only appropriate that the future reform agenda also include measures to protect intellectual property and address the problems identified on previous Special 301 reports that led to Ukraine's the Priority Foreign Country (PFC) designation. The software industry has been severely impacted by the difficult economic situation in Ukraine and it is important that, as reforms are implemented, intellectual property rights (IPR) protection improves.

Copyright

According to BSA's Global Software Survey, the estimated rate for unlicensed software use in Ukraine in 2013 was 83%, representing a commercial value of $444 million.[1]

Government Legalization: In 2015, the Government of Ukraine did not address the high level of unlicensed software use by government agencies. In addition, budget was not even allocated for software legalization.

The Government has engaged in regular discussions about unlicensed software use by government agencies but to date no government representative or agency has been given authority to take action in this regard. Most recently, the Ministry of Economic Development and Trade (MEDT) participated in relevant legalization discussions but so far, procedures have not been put in place to ensure a comprehensive and permanent shift in policies leading to government use of licensed software. In 2015, the State Intellectual Property Service (SIPS) initiated an internal software audit of government agencies, but unfortunately, the exercise was partial, resulting in incomplete reports on the level of unlicensed software use. Only a few central agencies located in Kiev were audited and software license checks were not executed at the regional levels.

Statutory and Regulatory Provisions: In August 2015, MEDT adopted a plan approved by the Prime Minister to reform the IPR protection system. This plan includes legislative amendments to improve the protection of IPR and to promote audits of software products used by state agencies, and legalization of software used by the public sector.

A draft law developed by MEDT with the input of some interested stakeholders (including the software industry), which would address copyright infringement over the internet and implement a notice and takedown system, was submitted to the Ukrainian Parliament in October 2015. Despite its overall positive nature, the draft contains several quite burdensome provisions that could in practice prevent 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.

implementation of notice and takedown system. For instance, the draft law establishes inadequate timelines for the completion of some actions related to the notice and takedown process (namely, some are too short, e.g. 24 hours for removing infringing content upon the right holder's notice; or too long, e.g. 10 to 14 business days for restoring improperly removed content). In addition, the draft contains a controversial provision targeted at preventing repeated uploading of illegal content, which appears to impose an onerous obligation on Internet Service Providers (ISPs) to monitor/filter the content. Mandatory use of digital signatures-also proposed by this draft law-would be unduly burdensome, considering that the procedure to obtain such signatures is quite complicated in Ukraine, especially for foreign companies. Finally, ISPs' obligation to provide users' personal information should be based on court orders, not on mere requests by an interested parties, as the current draft mandates. The draft law should, therefore, be revised to address these issues before it is adopted. Notwithstanding the submission of the draft law to Parliament as a governmental legislative initiative, the draft law has not been included in the parliamentary agenda so far.

Compliance and Enforcement: In 2015, the number of IP enforcement actions conducted by the Ukrainian police significantly decreased compared to previous years. For example, according to information available to BSA, in 2015 the police conducted 38 actions against commercial end-user companies suspected of unlicensed software use, and 27 channel raids were conducted against resellers suspected of distributing unlicensed software. These figures are much lower than the 56 criminal raids initiated against end-user companies and the 63 raids against resellers in 2014.

The new *"Prosecutor's Office Law"* and the *"National Police Law*" entered into force on July 15, 2015 and on November 7, 2015, respectively. According to the new legislation, regulations governing Ukrainian law enforcement authorities are undergoing substantial reform, including significant changes to the structure of both agencies. All existing staff are now tested and examined in order to ensure the selection of the most professional and reputable officers, as well as to reveal and disengage all personnel suspected of negligent or corrupt conduct. Moreover, the *National Police Law* provides for the creation of a special Cybersecurity Department with new staff and specific IPR online enforcement responsibilities.

Notwithstanding the intended positive goals of such reform, in practice, these laws are currently being used by officials to justify lack of action against copyright infringers because implementing measures have yet to be finalized. Overall, the trend is very concerning: ex-officio police raids continue to focus only on small targets, and police refuse to target any large companies. Most criminal cases initiated against IPR infringers are not concluded and very few result in criminal judgments. Several criminal complaints filed by a BSA members have been pending for years with no prospect of being transferred to court. Courts often refuse to issue search warrants for police to seize computers, which effectively stops any further investigation. Civil claims filed by right holders within criminal proceedings as is provided by the law, are often rejected by courts, forcing right holders to initiate separate, costly civil proceedings, which often are not concluded because civil ex parte searches are not available. Therefore, ineffective criminal proceedings are the only avenue for right holders to secure evidence and pursue actions against infringers.

The political turmoil has understandably contributed to inadequate protection of IPR in Ukraine. However, the poor state of IPR protection in the country is not only caused by the political situation and the lack of police motivation to address copyright offenses, but also by the absence of political will to encourage law enforcement authorities to take effective action in this area. An official action plan and clear instructions to promptly investigate and prosecute suspected IPR infringements, including distribution and use of unlicensed software, are urgently needed.

Lastly, in addition to the police, SIPS is formally empowered to investigate IPR infringements. However, in 2015, SIPS has not performed its duties due to a legislative moratorium on inspections of business entities. At the same time, the number of SIPS inspectors nationwide has decreased from 27 to 9, so it is anticipated that in the future SIPS will be even less able to execute its supervisory functions in the sphere of IP protection.

Recommendation: Due to the lack of any concrete positive changes to protect software copyrights, the absence of a tangible plan for software legalization in the public sector, and a significant decrease in enforcement activity, BSA recommends Ukraine be placed on the **Priority Watch List**.

VIETNAM

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

Overview/Business Environment

Vietnam has initiated institutional reforms over the last two years, some with potentially positive effects in the overall investment environment. Unfortunately, many measures for regulating the information technology (IT) sector are likely to reduce fair and equitable market access for BSA members wishing to provide software products and online services in Vietnam. Vietnam has recently adopted market access restrictions on server location and government procurement that threaten the ability of foreign IT service companies to compete in the marketplace. Although these measures are still in place, Vietnam's participation in the Trans-Pacific Partnership (TPP) is a positive development and will likely require changes in such polices. BSA receives good support from the Ministry of Culture, Sports and Tourism (MCST) and the High Tech Crimes Department of the Public Security Ministry (High Tech Police) in enforcing against the unauthorized use of software by enterprises in Vietnam. Unfortunately, the use of unlicensed software use remains very high, both in the private and public sectors.

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 not only hamper the ability of BSA members and others in the IT sector to provide innovative products and services to the Vietnamese market but they may also conflict with commitments to allow the cross-border transfer of information by electronic means under the TPP.

Information Security: Vietnam's legislative body, the National Assembly, enacted the Law on Network Information Security on November 19, 2015. Despite several submissions by BSA in the course of public consultation on the Law, it still contains numerous provisions that are of concern. The Law broadly obliges Internet Service Providers to coordinate with "competent State authorities" in handling and preventing online information security threats arising from Internet users, but there is a lack of clarity as to the scope of the required coordination. There are provisions that may limit the ability to provide encryption solutions for consumers and enterprises in Vietnam. The Law also includes an overly broad definition of "personal information" and appears to impose excessive consent and notification requirements. These provisions are likely to impact the ability of BSA members to provide on-line services in Vietnam.

Cross-Border Data Flows and Server Localization: On September 1, 2013, Decree No. 72 went into effect.[1] The decree imposes 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.

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

Specifically, Article 4.2.f of Circular No. 9, which implements certain provisions of Decree No. 72, requires general news website operators, social network service providers, search engines, and online applications to have at least one server system in Vietnam to allow for inspection, storage, and provision of information at the request of competent authorities.[2] In early 2015, the Government of Vietnam proposed to further elaborate these requirements in a Draft Circular. The Draft Circular also mandates companies providing certain online services to establish a local entity in Vietnam. These measures may impact the ability of BSA members to provide software-based services online (e.g., cloud computing), which offer many economic benefits, especially to small- and medium-sized enterprises in Vietnam. The 2015 Draft Circular has not yet been finalized.

BSA and our members raised renewed concerns regarding a revised Draft IT Services Decree (Draft Decree) issued in 2014 by the Ministry of Information and Communication (MIC) that regulates IT services in Vietnam. BSA filed comments in 2012 on an earlier version of this measure. We remain concerned about a number of elements in the Draft 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 international data transfers, impose unnecessary requirements to localize hardware (e.g., servers) in Vietnam, and require unwieldy certification requirements for IT service professionals, among other things.

Many of the requirements above appear to be incompatible with Vietnam's TPP commitments on cross-border data flows and server localization. For these reasons and others, BSA urges the government of Vietnam to reconsider these policies.

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.

[2] Ministry of Information and Communication's Circular No. 09/2014/TT-BTTTT: Detailing management, provision and use of information on websites and social networks (in force since October 3, 2014)

[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

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. Both the MCST and the High Tech Police are supportive of BSA efforts to enforce against the unauthorized use of software by enterprises in Vietnam, with administrative actions against such actors increasing from 34 in 2014 to 89 in 2015.

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code (as last amended in 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.

The Criminal Code, as currently in force, 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." However, there has been a general lack of criminal enforcement against copyright infringement over the years on the part of the authorities. Further, while Article 170a of the current Criminal Code 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]

In November 2015, the National Assembly adopted the new Criminal Code which will take effect on July 1, 2016. While the official text of the final new Criminal Code has not yet been made public, its "Final Draft" indicates improvements in provisions addressing copyright infringements. Under Article 226 of the Final Draft, demonstrating "commercial scale" copyright infringement would no longer be necessary for triggering a criminal offence. Furthermore, an organization that commits copyright infringement is now subject to criminal penalties and may be fined up to VND3 billion (~USD150,000) and its business operations may be suspended for up to two years. BSA urges the Vietnamese government to take the opportunity to increase its criminal enforcement efforts, particularly considering the heightened commitments made by Vietnam and other TPP parties regarding criminal enforcement of intellectual property rights.

---

[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.

[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]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.

Amendments to the Intellectual Property Code over the years have resulted in 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 caused by the infringement is difficult to calculate.

Compliance and Enforcement: BSA significantly relies on administrative enforcement to combat the unlicensed use of software by enterprises in Vietnam. However, fines remain too low to constitute an effective deterrent against future infringements. BSA is working in partnership with the Vietnam Copyright Office and the Inspectorate of the MCST to address the use of unlicensed software in Vietnam. The Partnership in Protection of Software Copyright was established in 2008. In 2015, 89 administrative enforcement actions were initiated. Unfortunately, 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.

While in 2015 BSA received good support from government agencies for a "National Crackdown Campaign," the lack of criminal enforcement against copyright infringement remains a concern. 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 current 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. Despite this, BSA brought two cases to civil court in 2015 and hopes that over time, civil remedies will be available to supplement administrative, and eventually, criminal enforcement.

Technical Assistance and Education: In 2015, BSA collaborated 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, and Ministry of Science & Technology. During the period of March 27 – April 30, 2015, BSA and the Task Force organized an Intellectual Property Day campaign, where both educational and enforcement campaigns were conducted.

Recommendation: Due to extremely high levels of unlicensed software use by enterprises and government institutions, the lack of criminal enforcement against willful use of unlicensed software by enterprises, as well as a number of increasingly troubling IT regulatory measures, BSA recommends that Vietnam be placed 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 remain 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. Brazil's current challenging political and economic situation--including rapidly rising inflation rates, declining exchange rates, and budget cuts--may affect initiatives to promote intellectual property, such as enforcement efforts. Discussions and implementation of relevant policies may also be delayed in 2016 as a result of the current political scenario in the country.

Market Access

The market access environment in Brazil for BSA members 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. 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 personal data protection regulation reflects 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 Personal Data Protection Bill to address outstanding aspects of personal data and privacy protection. There are currently multiple versions of the proposed regulation being drafted by the Executive (Ministry of Justice) and Legislative branches (Senate and Lower House) of the Brazilian Government.

BSA provided comments to the government of Brazil on both the proposed Personal Data Protection Bill that is being drafted by the Ministry of Justice and on a separate version of the bill which is being analyzed by the Brazilian Senate. Eventually, both texts are likely to be consolidated. BSA has been urging 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.

Although there have been improvements vis-à-vis initial drafts, the most recent draft of the Bill published by the Ministry of Justice and of the Bill under consideration by the Brazilian Senate still raise concerns. These concerns include extra-territorial reach of the Brazilian law, potential of explicit consent being required to legitimate a wide range of data treatment operations, restrictions on cross-border data flows, and unreasonable liability on data processors.

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 by May 2019.

The Ministry of Planning developed regulations to implement 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 regulations present multiple serious problems for BSA members, especially the deviation from global standards and requirements to disclose source code and other intellectual property. BSA provided the Ministry of Planning public written comments, which we submitted in late 2014, and met with the agency in early 2015. Despite BSA's efforts, this dialogue did not convince the Brazilian government to 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, 25 Brazilian companies have certified 28 software packages. Only two non-Brazilian companies have certified individual products; one of these companies acquired a Brazilian corporation and the product certified was part of the Brazilian company portfolio.

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 it was resubmitted at the beginning of the 2015 congressional session with a new favorable reports and a sponsor interested in forwarding the issue. 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.

Finally, the Brazilian Congress is currently discussing potential changes to Brazil's Procurement Law. The current law allows the public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of ICT systems to be limited to local goods and services only if such products and/or services are classified as "strategic" by a Decree published by the government. A bill currently pending Congressional approval could remove the need for such

classification. Should the bill be approved, any public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of ICT systems could be limited exclusively to local goods and services creating a market access barrier for foreign companies.

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 what has been 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 efforts in Brazil also include a comprehensive risk awareness communication campaign called Pensando Bem ('Think Again'). This campaign is conducted exclusively online and is a joint collaboration with the local software association, ABES. The campaign is meant to drive awareness of the risks of the use of unlicensed software while giving individuals the opportunity to proactively report unlicensed use.

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 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.

[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.

As the software industry transitions to subscription-based software services and continues to devise other innovative ways to meet customers' changing demands for software, such as leveraging cloud computing and other Internet-enabled data services, the ability to enforce software licensing in the digital environment will continue to be key. BSA and its members look forward to working with the Brazilian government to advance the enforcement of licenses in the digital environment.

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-counterfeiting and piracy campaign. The level of funding for the activities promoted by the agency is much lower than it used to be years ago. It is critical that CNCP be properly funded and that the agency continues to work closely with industry and vigorously follows up on initial steps to expand its work beyond its traditional focus on counterfeiting and piracy of physical goods.

Government Engagement: In 2014, BSA signed a cooperation agreement with the government of Santa Catarina state, which has agreed to support BSA's awareness raising efforts in that state. The government of 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. The engagement with the State government continued in 2015.

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 remain on the **Watch List**.

GREECE

Due to persistent and growing high levels of unlicensed software use in 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) member states, requiring urgent improvements to the legal framework in order to encourage 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 software and information technology (IT) 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 the responsibility of overseeing an audit of the government's use of software and the development of an awareness campaign to educate public officials about the risks associated with the use of unlicensed software. The adoption of effective, transparent, and verifiable software asset management procedures, through which government agencies conduct regular audits of the software they have installed to ensure, among other things, that all software in use is properly licensed, would also provide a powerful positive example to private enterprise.

Statutory and Regulatory Provisions: An amendment to the Greek Copyright Law which would include a provision entitled "Sanctions against Copyright Infringements over the Internet" is currently being considered. The proposed amendment 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. As currently written, the provision would not apply when end users download or stream infringing materials, or exchange infringing files through peer to peer networks. Cloud providers of data storage services are also out of the scope of the regulation. BSA urges the Greek government to continue working to pass legislation that properly balances the interests of copyright holders, users, and Internet Service Providers (ISPs).

[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.

Under current law, ISPs are not allowed to disclose the Internet Protocol (IP) addresses of their users who infringe copyrights. This prohibition hinders enforcement activities. An amendment to the current law has been proposed to allow the disclosure, based on a court order, of IP addresses or other personal data such as traffic and location data, when a copyright infringement amounts to a felony. The amendment would not affect copyright infringements considered misdemeanors. The passage of this amendment would be a positive development but it should include all copyright infringements (felonies and misdemeanors).

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 number of raids conducted in 2015 decreased in comparison with the previous year. In 2015, the Financial and Economic Crimes Unit (SDOE) conducted 6 raids, which resulted in the imposition of around 50,000€ 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 Special IPR and Electronic Commerce Department receives the funding and resources it needs to carry out its mission. It is also paramount that the Department recruits additional trained personnel in order to conduct more frequent inspections, building upon the good work performed in the past.

Inspections that were suspended in 2015 due to SDOE's reorganization should be rescheduled as soon as possible. The Special IPR Department should also resume issuing letters to companies requesting inventories of software in use and respective licenses and invoices. In addition, the agency should resume issuing follow-up warning letters in cases of non-responsive companies and conduct inspections, when appropriate, targeting such companies. The Special IPR Department should also readopt the practice of publishing the results of raids on its website and issuing public releases to raise public awareness. Furthermore, the Special IPR Department should more efficiently enforce the policy that inspectors check software license compliance, in addition to tax compliance, in daily tax inspections.

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, which entered into force on January 1, 2016, and 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. The changes in the Code of Civil Procedure are intended to expedite Court procedures. However, it is not clear whether the special intellectual property departments within the Civil Courts of First Instance of Athens and Thessaloniki, and within the Court of Appeals of Athens will be maintained. These departments are staffed with experienced and qualified judges and it is crucial that they are kept to ensure the benefits of the new Code of Civil Procedure are fully leveraged.

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 persistent and growing high levels of unlicensed software use in 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 Kazakhstan be placed on the Watch List.

Overview/Business Environment

The overall business environment for the software industry in Kazakhstan remained largely unchanged in 2015. According to the most recent data, the rate of unlicensed software installation in Kazakhstan has dropped only marginally from 76% in 2011 to 74% in 2013. This represents a commercial value of US$136 million in unlicensed software.[1]

Kazakhstan was admitted to the World Trade Organization (WTO) in November 2015 after lengthy negotiations with WTO members. It is clear from the Working Party Report and Protocol that Kazakhstan has committed to be compliant with WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) from accession, which includes intellectual property rights (IPR) enforcement commitments. IPR enforcement is an issue that will continue to be the subject of scrutiny as the US Administration and Congress deliberate on the granting of Permanent Normal Trade Relations to Kazakhstan.

Concrete progress has been insufficient due to lack of enforcement. Many issues remain unchanged, in particular because the initiatives proposed in the IPR plan are not fully supported by state officials.

Copyright and Enforcement

BSA's primary concern in Kazakhstan remains the significant volume of commercial entities that persist in using unlicensed or under-licensed software.

Government officials in Kazakhstan, as a result of right holders' efforts, continue to gain a better understanding of the risks involved in using unlicensed software and the importance of intellectual property to the economy. In particular, the Council for Improvement of the Investment Climate, chaired by the Prime Minister and consisting of representatives of various state agencies and foreign investors, created a special IPR working group of which BSA is a member. A number of recommendations have been submitted by BSA to the working group. Unfortunately, concrete improvement to IPR protection has not been achieved.

Statutory and Regulatory Provisions: The Criminal Code provides police with ex officio authority to commence criminal copyright cases, but it is not used against commercial end-user companies suspected of unlicensed software use. In addition, Article 198 of the Criminal Code, which establishes criminal liability for IPR infringement, has limited impact because of unclear wording of the relevant provision. The text could be interpreted to only refer to the manufacturing and sale of illegal software, while end-user cases (i.e. those involving reproduction and use, not sale or manufacturing, of unlicensed software) would remain unaddressed by the provision. As a result, the police routinely refuse to initiate cases against such end-users, to perform inspections and/or to secure the necessary evidence of unlicensed software use. This situation, combined with vague and inefficient *ex parte* search provisions in the civil legislation, has led to inability of software right holders to take effective action against suspected

[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.

infringers either based on criminal or civil law, since without a criminal or civil search it is nearly impossible to secure the needed evidence of unlicensed software use.

Compliance and Enforcement: The law enforcement agencies responsible for IPR enforcement in Kazakhstan, the Ministry of Interior, and the Agency of State Income under the Ministry of Finance, have achieved some results related to IPR protection in the country.

However, in practice, the actions undertaken[2] by the agencies above mentioned have not impacted the high level of unlicensed software use in the country. These actions have not addressed the root of the problem, which continues to be the widespread use of unlicensed software both by government organizations and commercial businesses. The number of enforcement actions conducted by Kazakhstani law enforcement bodies against enterprises that infringe upon BSA members' software copyrights dropped from 323 in 2013 to 51 in 2014, and further to six in 2015. Out of these six actions, only one has resulted in a decision against the infringing company. Criminal investigations have not been an effective mechanism to address the use of unlicensed software by enterprises either. Out of 14 investigations launched in 2015, only one resulted in criminal charges and two cases were settled. The remaining cases remain under investigation.

Positive steps to address the high level of unlicensed software use in the Kazakhstan should include law enforcement capacity building, the establishment of a specialized agency dedicated to enforce IPR, the use of global best practices to advance IPR enforcement, and the implementation of obligations arising from international IPR agreements (WTO TRIPS agreement).

Government and SOE Licensing/Legalization

The Ministry of Justice has taken a leadership role in promoting the importance of licensed software use by government agencies in order to prevent serious cybersecurity risks. However, the use of unlicensed software by government agencies remain a concern. Weaknesses in the public procurement process have also resulted in a high volume of unlicensed copies of software being acquired by government agencies. The newly updated law on Government Purchases became effective on January, 1 2016. As a result, BSA remains hopeful that the government will establish and implement new provisions to regulate the acquisition and management of software by the government. The adoption of effective, transparent, and verifiable software asset management procedures, in which government agencies conduct regular internal software audits to ensure they use only licensed software, would 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 Kazakhstan be placed on the **Watch List.**

[2] Activities include raids targeting sellers of unlicensed software and other products, IPR seminars and training programs, and broad IPR awareness campaigns that did not specifically address the use of unlicensed software by enterprises.

REPUBLIC OF KOREA

Due to an increasingly difficult market access environment for software and information technology (IT) products, ongoing concerns related to government use of unlicensed software, and a decrease in software license enforcement activities, 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 software and information technology (IT) sector as a whole, is mixed. Korea has a strong IT 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 software and IT products. 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. Although the Cloud Computing Promotion Act came into force on September 28, 2015, it remains difficult to provide cloud-based services to the Korean market. Data residency and other requirements for sectors such as government/public services, finance, healthcare, and education exist which hampers the ability to provide cloud-based services to users in these sectors. In addition, the actions of the Korea Fair Trade Commission raise serious concerns about whether foreign companies in Korea will be treated fairly in their investigations.

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 enforcement actions 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. Furthermore, due to procedural impediments such as the lack of an effective discovery system, low damage awards, and a reluctance to issue preliminary injunctions, civil courts are not very effective in addressing software copyright infringement cases.

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-computing and data analytics services, in Korea.

Cross-Border Data Flows and Server Localization: Although the Cloud Computing Promotion Act came into force as of September 28, 2015, the National Intelligence Service (NIS) has still maintained the position that many public sector entities should not use commercial cloud services without following specific NIS guidelines, including guidelines requiring internal systems to be physically or virtually

separated from public-facing systems[1]. Similar guidelines and regulations requiring network separation and/or data on-shoring exist in the context of the finance[2] and healthcare[3] sectors. We are concerned that, even after enactment of the Cloud Computing Promotion Act, significant barriers still exist to cloud service adoption.

KFTC's Intellectual Property Abuse Guidelines: On 17 December 2014, the Korea Fair Trade Commission (KFTC) issued amendments to the "Guidelines for Examination of Improper Exercise of Intellectual Property Rights" ("Guidelines"). The Guidelines were promulgated in final form and entered into effect immediately. The Guidelines are intended to clarify "abuse" of intellectual property rights (IPR) in the context of competition policy. Of particular concern, the Guidelines establish the concept of "de facto standard essential patents (SEPs)." On a positive note, BSA was encouraged by the steps that the KFTC took in December 2015 regarding the Guidelines, including the solicitation of public comments to revise them. BSA looks forward to an early resolution of this issue. It is paramount that the Guidelines are modified so that the definition of SEP and standard technology clearly excludes any technologies or patents for which there has been no voluntary licensing commitments in the context of industry-led collaborative standards development.

Lack of Transparency and Procedural Fairness in KFTC Antitrust Investigations: BSA is concerned that, when conducting antitrust investigations, KFTC appears to operate with insufficient transparency and predictability and does not consistently operate in a manner that comports with due process and procedural fairness to the firms under investigation. For example, BSA has received reports that not all evidence might have been shared with firms under investigation, that firms under investigation might not have received full access to key witness, and that witnesses might have felt pressured under investigations.

Furthermore, KFTC's caseload, which includes at least 40 antitrust investigations against US companies in the last four years, appears to show a concerted effort to prioritize antitrust investigations against US companies. The KORUS FTA includes provisions addressing competition related matters. The relevant chapter (Chapter 16) sets forth significant antitrust-related obligations for the parties, including specific due process provisions and procedural safeguards, guaranteeing parties the right to cross-examine witnesses and review all documents on which charges are based. Furthermore, Article 16.1(2) of the FTA, provides that "the enforcement policy of each Party's [competition] authorities responsible for the enforcement of such laws is to treat persons who are not persons of the Party no less favorably than persons of the Party in like circumstances, and each Party's authorities intend to maintain this policy." BSA is concerned that the recent behavior of the KFTC in investigating US companies appears to be inconsistent with many of these obligations.

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 applied to locally-certified products. In 2014, the Korean government extended similar security-conformity testing requirements to international Common Criteria-certified

[1] The Network Construction (Separation) Guidelines.

[2] E.g., under the Financial Services Commission's 2013 Regulation on the Supervision of Electronic Financial Activities (Supervisory Regulation).

[3] E.g. under the Medical Services Act.

networking products for all central government agencies. In 2016, the government is expected to further extend the policy to all public organizations, local governments, and other government-related agencies, such as educational institutions. In combination, Korean government agency procurement authorities have interpreted these policies as requirements to buy local IT products and to avoid foreign products, although such interpretation has never been reduced to writing. 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, including in KORUS. Although BSA and other organizations have raised this issue several times with the Korean government, the issue remains unresolved at this time.

Procurement Preferences: The current administration has adopted a number of policies to promote small- and medium-sized enterprises (SMEs). We urge the Korean government to avoid such procurement preferences, whether based on licensing models or on the nature of the supplier. Such policies 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.[4] 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. Efforts by some agencies unfortunately are not being replicated by other ministries and agencies where unlicensed software continues to be an issue. BSA requests that USTR open up a dialogue with relevant representatives of the Korean government to

[4] 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.

identify a mechanism to address this challenge and to ensure Korea's full compliance with its commitments under the KORUS.

Compliance and Enforcement: Criminal enforcement has been an effective mechanism for BSA members to protect their rights and enforce 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 enterprises using unlicensed software. This force, however, has limited resources and BSA members also rely on the enforcement actions of the police.

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. 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 30 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. In 2016, Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules allowing rights holders to effectively seek civil remedies against software copyright infringement.

Recommendation: Due to an increasingly difficult market access environment for software and IT products, ongoing concerns related to government use of unlicensed software, and a decrease in software license enforcement activities, BSA recommends Korea be placed on the **Watch List**.

MEXICO

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

Overview/Business Environment

The rate of unlicensed software use in Mexico 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 online. Concerns about unlicensed software use by enterprises and about judicial enforcement mechanisms are ongoing. 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 should be an ongoing effort for all governments. Mexico has been a global leader 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.

[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.

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 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. One enforcement officer has recently been assigned to each of IMPI's regional offices in Guadalajara and León and these officers are soon expected to begin conducting audits that will aid enforcement procedures locally. In 2015, IMPI brought 1,507 actions against enterprises using unauthorized software (1,162 *ex officio* actions and 345 *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. A final ruling on a typical intellectual property infringement case brought to court after an administrative proceeding is concluded is likely to take at least 10 years. Judicial procedures need to be shorter with 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 has been difficult to address because of the lack of basic investigative and prosecutorial tools. However, the recent creation of a cybercrime division within the Attorney General's Office (PGR) is a positive development and should improve the current scenario. A dedicated group of prosecutors and investigators working exclusively on cybercrimes should increase efficiency of investigations. It is also worth highlighting that in order to comply with its Trans-Pacific Partnership obligations, Mexico is likely to soon implement a notice and takedown system to address cooperation between intellectual property rights (IPR) holders and Internet Service Providers (ISPs) to address online IPR infringement.

The requirement to have expert opinions for every software infringement criminal case, as well as to provide physical copies of legal and illegal software, complicates criminal prosecution. These requirements have a historic root but they need to be changed drastically to adjust PGR's practices to current technology. This is a good time to carefully consider and implement these changes because the criminal system is currently undergoing a transition and many changes in criminal prosecution procedures are taking place.

PGR has re-launched the Interinstitutional Committee for the Protection of Copyrights and IPRs, and has proposed that the public, private, and academic sectors, as well as the civil society, execute a new National Agreement for the Protection of Intellectual Property at the highest executive levels, with the participation of the President of Mexico.

Technical Assistance and Education: During 2015, 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 Certified Public Accountants, chambers and associations, entrepreneurs, students, customs agents, importers, and exporters. The program topics included intellectual property rights, software protection, innovation, cybersecurity, ISP liability, software

related tax matters, Verafirm certification, customs enforcement, licensing, administrative practices, notorious markets, rule of law, and accounting practices.

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

NIGERIA

Due to guidelines that if fully adopted would make Nigeria one of the most restrictive and closed markets for software, IT hardware, and services, BSA recommends Nigeria be placed on the Watch List.

Overview/Business Environment

As the largest economy in Africa, Nigeria presents significant opportunities for global information technology (IT) companies. The country's IT 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 IT-enabled growth a top priority and is actively seeking to build a viable, domestic IT and telecommunications sector.

In 2014, the Nigerian government released the Guidelines for Nigerian Content Development in Information and Communications Technology (Guidelines). The Guidelines were then issued in revised form in November 2015 by the Buhari Administration, which announced that the government would begin enforcing implementation immediately for all multinational IT companies. If the Guidelines are fully implemented, Nigeria would become one of the most restricted and closed IT markets in the world. Specifically, the Guidelines impose stringent local content requirements for IT 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.

As noted above, the Buhari Administration has announced its intention to begin immediate implementation of the Guidelines, despite the concerns of US companies and the US Government. BSA member companies report that in November 2015, the Nigerian government demanded that US companies prepare and submit within 30 days a detailed "implementation plan."

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 IT 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 software, IT hardware, and services. Section 10.1 requires manufacturers to obtain certification that IT hardware has been assembled in Nigeria and requires 50 percent of "local content either directly or through outsourcing to local manufacturers." These requirements are not limited to IT 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 World Trade Organization'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 IT 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 guidelines that, if fully adopted, would make Nigeria one of the most restrictive and closed markets for software, IT hardware, and services, BSA recommends Nigeria be placed on the **Watch List**.

[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.

ROMANIA

Despite cooperation by Romanian government authorities on education and awareness endeavors, the lack of prioritization of copyright enforcement in Romania - particularly in the last 18 months - and persistently high levels of unlicensed software use by enterprises lead BSA to recommend Romania be placed on the Watch List.

Overview/Business Environment

The commercial environment for the software sector in Romania 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]

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

The new Criminal Procedure Code provides that only certified specialists may inspect computers during investigations of suspected unlicensed software use. As a result, economic police officers who previously conducted these inspections are no longer permitted to do so. Instead, the inspections must be performed exclusively by the limited number of certified specialists in the organized crime units of the police or by the Romanian Copyright Office (ORDA), which has only nine inspectors. This change in procedure significantly impedes enforcement efforts, as the number of organized crime officers available for inspections is considerably lower than the current number of economic police officers with the knowledge and skill to conduct such inspections. The manner in which the forensics analyses are presented frequently lack clarity and essential information, such as type, version, or edition of software programs installed or stored. This results in a substantial decrease in the quality of evidence in software copyright infringement cases. In sum, the lack of specialists and the often weak specialist reports result in a profound decrease in the total number of cases.

An amendment to the Criminal Procedure Code has been proposed which would allow economic police officers to also conduct inspections. Due to the long period of time that has elapsed (more than 18 months) from the date of its proposal, it is unclear if the amendment will be adopted.

Amendments to the Copyright Law are also being considered in Romania. These amendments could 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 amendment

[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.

should also correct the allocation of competence of copyright crimes to the Courts of First Instance, which has negatively impacted copyright enforcement cases. Prior to 2010, the competence for prosecuting and trying intellectual property crimes resided with 42 tribunal courts and their associated prosecutors' offices, where trained prosecutors and judges could focus on software infringement and other such cases. In 2010, this competence was shifted to as many as 188 generalist courts and their respective prosecutors' offices throughout the country. The lack of experience and knowledge of copyright matters by these generalist courts 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 three years.

Government Licensing/Legalization: BSA is increasingly concerned that efforts by the central government to ensure that government agencies use only licensed software have not progressed. The Romanian Government should take steps to ensure that all government agencies are using licensed software in accordance with the license terms and conditions.

Compliance and Enforcement: In 2015, Romanian law enforcement conducted 83 inspections of enterprise end-users and 6 distribution channel raids in which unlicensed BSA member software were found. There were nine convictions reported by BSA members in 2015. Moreover, out of the 89 raids in 2015, 55% were conducted in respect of low-profile targets (i.e. those with only one PC).

While authorities were active in partnering with BSA on education campaigns, enforcement actions have seriously declined over the last years. 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, with the support of the General Inspectorate of Police, the General Public Prosecutor's Office (GPO), and the Romanian Copyright Office, organized a series of 8 trainings, in the period of May-June 2015, for more than 150 law enforcement personnel. The trainings focused on the new legislative challenges, as well as on new technologies. Despite the personal involvement of high level officials, the trainings have yet to have any practical impact. There is a high rate of prosecutor turnover and they fail to support search warrants requests in intellectual property right infringement cases; on the rare occasion a search is executed, the evidence collected from computer searches continues to be substandard and often useless.

Recommendation: Despite cooperation by Romanian government authorities on education and awareness endeavors, the lack of prioritization of copyright enforcement in Romania - particularly in the past 18 months - and persistently high levels of unlicensed software use by enterprises lead BSA to recommend Romania be placed on the **Watch List**.

THAILAND

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

Overview/Business Environment

Thailand's software market did not significantly improve in 2015 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.

In 2015, Thailand's Securities and Exchange Commission (SEC), an independent public-sector regulatory agency, adopted software asset management (SAM) practices based on International Standards Organization (ISO) SAM standards. Other government agencies and private sector companies may follow this important lead, which is a positive development and may help reduce the use of unlicensed software. Unfortunately, the Royal Thai Government (RTG) lacks clear goals and strategies to reduce unlicensed software use by enterprises and has generally 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 enterprises. Instead, the bill includes broad exceptions and insufficient protections for rights management information (RMI) and technological protection measures (TPMs) which BSA members use to deter unauthorized and illegal use of their products and services.

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 appreciates the opportunities to discuss and address concerns in these bills, particularly the Ministry of Information and Communication Technology (MICT)'s Electronic Transactions Development Agency (ETDA)'s willingness to discuss the draft Personal Data Protection Bill. BSA urges the RTG to continue to conduct and enhance 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 Assembly of Thailand (NLA).

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 other technology sector companies to provide innovative and effective information technology (IT) products and services, including software.

Security: MICT, under the new Minister's direction, is reviewing the draft National Cybersecurity Bill. The draft Bill is designed to strengthen the cybersecurity capabilities of government agencies and provide

appropriate breach notification procedures. The draft Bill, 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 in Thailand.

Privacy: The draft Personal Data Protection Bill (draft PDP Bill) is also under review by the MICT. The draft PDP Bill is designed to build public trust and confidence in IT 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 March 2015, and held a number of meetings with the RTG where we highlighted the importance of protecting personal information and preventing misuse of such information for fostering the trust and confidence necessary for growth of the digital economy. However, BSA notes that the draft PDP Bill contains imprecise or unclear provisions in some cases, and in others appears to take an overly prescriptive approach that does not adequately take into consideration the nature of the personal information in question. Such an approach is not consistent with the expected technical and commercial 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 widespread adoption of digital products and services in the economy.

Copyright and Enforcement

BSA enjoyed good cooperation with the RTG authorities in 2015, including with the Economic Crime Division, in addressing the unlicensed use of software in Thailand. The latest figures, however, indicate that the rate of unlicensed software use in Thailand 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 procurement, installation, and use in the public sector remains a problem for BSA members. The use of unlicensed software may expose the RTG to unnecessary cybersecurity risks[2]. BSA urges the RTG to upgrade their networks and eliminate the use of unlicensed software to help reduce cybersecurity risks.

Statutory and Regulatory Provisions: The RTG amended Thailand's Copyright Law in 2014. Unfortunately, BSA's comments were not addressed in the final legislation. The new Copyright Law fails to provide effective remedies against the trafficking and distribution of devices and technology designed for the purpose of circumventing TPM and includes onerous requirements on the copyright owner to prove the intent or knowledge of suspected TPM circumvention that will hamper enforcement efforts. BSA is also 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.

[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.
[2] The "*Unlicensed Software and Cybersecurity Threats*" report available at http://bsa.org/malware demonstrates the link between unlicensed software and malware on personal computers (PCs).

Compliance and Enforcement: Thailand has a specialized intellectual property court, which has improved the effectiveness of intellectual property litigation in Thailand. 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 engaged with several RGT agencies to ensure the adequate protection for IPRs in the software industry and sound policies and legislations to promote the data driven economy and Thai Digital Economy initiatives. Those agencies include the Department of Intellectual Property (DIP), the Economic Crime Division, the Central Intellectual Property and International Trade (IP&IT) Court, and ETDA.

Technical Assistance and Education*:* BSA continued its SAM campaign in 2015. This campaign gained visibility when Thailand's Securities and Exchange Commission (SEC) and Thai Yamaha Motor Co., Ltd successfully benchmarked their SAM practices against the ISO 19770-1 SAM standard and achieved Verafirm certification from BSA. In several programs over the summer, BSA introduced the concept of SAM practices based on the ISO standard to over 30 enterprises. BSA explained the benefits of SAM for saving IT costs, reducing cybersecurity and legal risks, and enhancing corporate governance, and explained in detail how to establish the policies, processes and procedures of SAM. BSA also provided its online SAM course to a number of organizations during 2015. BSA is encouraged by the increasing number of enterprises in Thailand that are interested in SAM practices. If many actually implement these effective SAM practices, this may also help reduce the use of illegal and unlicensed software in Thailand, among the many other benefits to the companies and to Thailand's economy in general.

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

TURKEY

Based on Turkey's failure to fully 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 remain 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 eight years later, the government of Turkey has yet to fully implement the circular. As a consequence, unlicensed use of software within the government and in state-owned enterprises (SOEs) remains rampant. In 2016, 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 software and information technology (IT) industry.

Statutory and Regulatory Provisions: Turkey has been developing draft amendments to the Law on Intellectual and Artistic Work for the past several years. In 2015, the government of Turkey announced plans to amend its Patent Law. 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.

[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).

Compliance and Enforcement: 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. 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 fully 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 remain on the **Watch List**.

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 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 (SMEs) 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 2013, 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 may decrease due to the enactment of the new Criminal Code that came into force on July 1 2015. The new Criminal Code makes intellectual property crimes (including copying software without authorization and accessing unlicensed software) one of the offenses that triggers the corporate criminal responsibility response. This will make both companies and their managers criminally liable for the unlicensed copying of business software within information and communication technology systems of enterprises. However, the recent publication of Instruction 8/2015 by the General Prosecutor of Spain may hamper the positive effects these changes introduced by the Criminal Code could promote (please refer to next section for further details).

Statutory and Regulatory Provisions: In 2014, Spain enacted a set of reforms to the Intellectual Property Law and the Civil Procedure Law which went into force in early 2015. Amendments to the Criminal Code went into effect on July 1, 2015 but the effectiveness of some of these amendments may be jeopardized by recent policy developments in Spain.

Revisions to the Intellectual Property Law (Law 21/2014) were adopted and published on November 5, 2014 ("2014 amendments") and went into effect 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 actions against online infringers. For example, Article 158 describes the requirements with

[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.

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.

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 to obtain the identity of infringers, as preliminary evidence, prior to the formal initiation of a civil suit. There is also subject to certain limitations.

Recent amendments to the Criminal Code, which went into force on July 1, 2015, allow Spanish law enforcement to take criminal actions against enterprises that are willfully using unlicensed software. The amendments were approved by the Parliament in March 2015, and have been in force since July 1, 2015. These amendments overrode former 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 meets the standard for criminal prosecution. The former instructions resulted in a cessation of criminal enforcement actions against illegal file sharing and eliminated the possibility of prosecuting infringing enterprises.

Unfortunately, a new instruction issued by the Attorney General's Office (Instrucción 8/2015 de la Fiscalía General del Estado) on December 21, 2015, jeopardizes the positive effects of the changes implemented by the new Criminal Code. The new instruction establishes that the lack of license to use software remains insufficient to characterize unlicensed software use as a criminal offence, despite the amendment introduced by the Criminal Code. Therefore the positive amendments to the Criminal Code may not effectively deter the use of unlicensed software.

Other shortcomings in Spain's legal framework remain. Further 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 and ensure that the provisions function as intended to effectively enable the prosecution of manufacturers and distributors of circumvention devices.

A step in the right direction was an amendment to the Criminal Code (article 270.6 of the new Criminal Code), including a definition of TPM circumvention measures. The new Criminal Code considers the "manufacturing, importing into Spain, making available or possessing with commercial purposes any device conceived, produced, adapted or created to suppress or neutralize any technical device designed to protect software or any other copyrighted work" a criminal offense. This could help the courts issue more favorable interpretations but the fact that the expression "with commercial purposes" has been included may cause some misinterpretation by the courts to remain.

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: In March 2015, BSA and the Ministry of Industry signed a cooperation agreement through which the Spanish Government fully commits to promote awareness messages about the importance of legal software use, and the legal and technological risks created by unlawful software use. As result of this agreement, several awareness initiatives have been identified. The

first initiative under the scope of the agreement is underway and consists of a letter which is being sent jointly by the Ministry, BSA and AMETIC (local IT association) to nearly 19,000 companies and organizations throughout Spain. New initiatives resulting from the agreement are likely to take place in 2016 but they may be impacted by the results of the general elections that took place in Spain on December 20, 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**.