

20 F Street, NW
Suite 800
Washington, DC 20001

p.202/872.5500
f.202/872.5501

August 10, 2012

The Honorable Victoria Espinel
United States Intellectual Property Enforcement Coordinator
Office of Management and Budget
Executive Office of the President

Re: Request for Written Submissions from the Public
Concerning Development of the Joint Strategic Plan on
Intellectual Property Enforcement
77 FR 42766

Dear Ms. Espinel:

The Business Software Alliance (BSA)¹ appreciates this opportunity to provide comments concerning the second Joint Strategic Plan that your office is developing in accordance with the Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403 (Oct. 13, 2008). The Business Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of nearly 100 world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.

The Impact of Software Theft

Software drives productivity and innovation in almost every economic sector, helping businesses of all sizes perform better in good times and bad. It makes our lives easier and more connected. It can educate, entertain and inspire. Our industry is dynamic, innovative, and a powerful engine for job creation and economic growth. It is also critically dependent on intellectual property protection. It is no accident that the software industry was born in this country. America's enthusiasm for technology, combined with its effective and constitutionally rooted system of IP protection, served as the foundation for US leadership in this field.

The software industry sits at the center of a vibrant IT economy – a virtuous circle that is producing jobs and economic growth, spawning new enterprises, and bringing innovative technologies to consumers.

¹ BSA's members include: Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Intel, Intuit, McAfee, Microsoft, Minitab, Progress Software, Quest Software, Rosetta Stone, Siemens PLM, Sybase, Symantec, The MathWorks, and Trend Micro.

One major problem stands in the way of increasing our exports and expanding this ecosystem: software theft. In 2011, more than \$63 billion worth of software was used illegally on PCs around the world.²

In the US alone, just under one in five PC applications installed last year were unauthorized and unpaid-for – and we have the lowest software piracy rate in the world.³ Many of the world's fastest growing economies are plagued with massive illegal use of software. China, for example, has a PC software piracy rate of 77%. Russia and India have software piracy rates of 63% and Brazil's piracy rate is 53%. Even Western European markets such as France, with a 37% software piracy rate, are not immune to this problem.⁴

Most software theft occurs when an otherwise legitimate business makes illegitimate copies of software for its use. When repeated millions of times by businesses or consumers throughout the world, this conduct has a staggering cumulative effect. Software theft on the Internet is also a serious and growing problem.

Massive theft harms software companies, depriving them of revenue that could be invested in new products and services. The impact on the software industry in the US is particularly severe for the simple reason that the US is the leading player in the global software market.

Business software is a critical input of production for enterprises across all sectors of the US and global economies.

- It is used by firms along with other inputs to produce a broad range of goods and services.
- It helps increase productivity by helping coordinate the inputs used in the production process *within* a firm.
- It helps boost GDP growth by increasing coordination *across* firms, industries and government.

That is why the impact of software piracy has broad reaching consequences well outside of the software industry itself. When businesses in high-piracy countries disobey the law and steal the software they use to run their companies, they gain significant productivity and other benefits – but they avoid a cost that their law-abiding US competitors pay. When the products of companies engaging in software theft enter the US market, they are competing unfairly with those US producers, undermining sales of US goods and displacing American jobs. This problem is repeated in every country where US businesses – in all economic sectors – compete against companies that use stolen software to reduce their costs of doing business.

² Ninth Annual BSA and IDC Global Piracy Study (2012), available online at <http://portal.bsa.org/globalpiracy2011/> (hereinafter "2012 Piracy Study"), at 1.

³ *Id.* at 6. Although, at 19%, the US piracy rate is the lowest in the world (and the lowest we have ever measured it), the commercial value of pirated software in the US tops the world at \$9.8 billion. This is a function of the size of the US market.

⁴ *Id.*

The First Joint Strategic Plan

The Administration's first Joint Strategic Plan, released in June, 2010, has brought about significant progress in improving IP protection and enforcement in the US and globally. Key accomplishments include:

- Renewed efforts to improve IP protection in China, with a focus on achieving measurable progress;
- Issuance of guidance on technology neutrality in the acquisition of software to senior procurement executives and agency CIOs;
- Establishment of action plans with countries on Special 301 lists;
- Establishment of formal interagency IPR teams in US embassies in 17 countries;
- Establishment of voluntary practices by payment processors to stop doing business with pirates and counterfeiters; and
- Establishment of voluntary best practices to address online piracy and counterfeiting by Internet advertisers.

BSA appreciates the careful thought that went into developing the first Joint Strategic Plan and all of the hard work by multiple agencies that has gone into its implementation. These initiatives should continue and thus serve as a solid foundation on which to construct the second Joint Strategic Plan.

Strategy Recommendations: Specific Recommendations for Improving IP Enforcement Efforts

A. Require Federal Contractors to Use only Licensed Software

In our submission to this office during the development of the first Joint Strategic Plan we identified elimination of the use of unlicensed software by federal contractors as an important means of reducing software theft and setting a good example for the rest of the private sector. We observed that

In the US, the federal government can have a profound effect on reducing software theft, not only through its direct procurement of software, but also by leveraging its role as a procurer of other goods and services. The principle established by EO 13103 can be extended by executive order to require that federal contractors also use only legal copies of software. Firms that seek to sell goods and services to the US government should certify that their use of software is in compliance with the Copyright Act and relevant license agreements, and that they have controls in place to ensure that this is the case. By extending the executive order in this way, the Administration would establish a standard for other governments to follow.

BSA appreciates the Administration's ongoing work on this issue. Nevertheless, as the experience of our member companies has demonstrated, use of unlicensed software by federal contractors remains a problem. For example, BSA recently analyzed our enforcement actions on behalf of our member companies. That analysis found that more than 25 percent of BSA's US enforcement actions in a two-

year span were against registered government contractors. More recently, BSA reached a settlement with a major US defense contractor for \$625,000 to settle claims that the company had unlicensed copies of member company software on its computers. Based on these continued cases, BSA renews its earlier call for formal executive action to ensure that use of unlicensed software by federal contractors is not tolerated.

B. Establish the Federal Government as a Model for Using Only Properly Licensed Software and Complying with License Terms

Executive Order 13103 has been instrumental in promoting the use of licensed software in Federal agencies in accordance with license terms. As the introduction to the 1998 Executive Order stated:

The United States Government is the world's largest purchaser of computer-related services and equipment, purchasing more than \$20 billion annually. At a time when a critical component in discussions with our international trading partners concerns their efforts to combat piracy of computer software and other intellectual property, it is incumbent on the United States to ensure that its own practices as a purchaser and user of computer software are beyond reproach.

Today, the US Government remains the world's largest customer for computer-related services and equipment, with an overall IT budget of approximately \$78 billion. Yet around the world, end-user piracy by governments and government enterprises remains a persistent source of harm to US software developers, job creation and US economic growth. In this environment, it is more important than ever that Federal agency heads and chief information officers lead by example to develop and implement effective practices consistent with those required by Executive Order 13103.

The IPEC can play an important role in encouraging the development of best practices to ensure that US agencies follow the guidance in the Executive Order, secure appropriate software licenses, follow license terms, and carry out prompt remediation in cases, if any, where their efforts fall short. IPEC leadership in pursuing the interagency exchange contemplated by section 3 of the Executive Order and in seeking regular dialogue with rights holders would be welcome.

C. Continue to Press for Measurable Progress against Software Theft in China

As noted above, BSA appreciates the efforts made over the past several years to tie progress on software legalization and IP protection in China to measurable benchmarks such as increased legal software sales. We look forward to continuing to work with the US government to supply appropriate metrics by which progress can be measured and evaluated.

At the same time, we urge the US government to continue press the Chinese government in the Joint Commission on Commerce and Trade (JCCT), the Strategic and Economic Dialogue (S&ED) and other appropriate venues to undertake measures to increase legal software sales. These include:

- Fulfilling its commitments on government software legalization in a comprehensive and transparent manner that utilizes software asset management (SAM) best practices;
- Implementing a comprehensive software legalization program for the state-owned enterprise (SOE) sector, including ISO-compliant SAM practices;
- Reforming its Copyright Law, Criminal Code and related laws and judicial interpretations (JIs) that are currently under review to facilitate civil and criminal enforcement against software piracy; and
- Eliminating “indigenous innovation” policies that compel transfers of IP to access the market

D. Encourage Voluntary Measures to Help Address Online Infringement

BSA is grateful for your leadership in facilitating dialogue aimed at the development of industry best practices to curb online infringement. We believe that voluntary industry agreements and industry best practices have the potential to play an important role in ongoing efforts to combat online piracy more effectively.

As you are well aware, individuals who engage in online piracy will adjust their sales and distribution tactics as necessary to circumvent obstacles that would otherwise impair their ability to profit from their illegal activities. To ensure that progress continues as online infringers adapt to evade detection and rights holder mitigation efforts, we encourage the government periodically to convene multi-stakeholder meetings to identify emerging threats and challenges.

We also believe that right holders themselves have a role to play in ensuring that best practices in connection with currently available enforcement mechanisms are followed. We therefore urge the IPEC to advance a dialogue among interested parties aimed at developing best practices for the submission of take-down notices under the Digital Millennium Copyright Act. Optimizing the notice procedures available under the DMCA will give us a clearer picture of the areas in which new voluntary practices might be warranted.

E. Continue to Improve IP Protection and Enforcement Overseas through Trade Tools

The US government has a number of trade tools at its disposal to persuade our trading partners to improve levels of IP protection and enforcement. In its new Joint Strategic Plan, the Administration should continue to seek ways to improve the effectiveness of these tools.

Special 301: The Administration’s first Joint Strategic Plan included measures to improve the effectiveness of the Special 301 program, which is one of the most important (as well as one of the oldest) of these trade tools. BSA applauds these actions. In addition, we recommend that the Administration consider updating the Special 301 criteria to take express account of persistently high piracy rates in making determinations under the statute.

Existing Trade Agreements: In addition to IPR provisions, there are other provisions of trade agreements that potentially could be used against countries that tolerate high levels of IP theft. For example, software theft distorts competition and confers

an unfair advantage on companies that engage in illegal activity. A government that permits theft of software by companies operating within their borders is effectively subsidizing the goods and services that those companies produce and export.

New Trade Disciplines: The US government is in the midst of negotiations for a Trans-Pacific Partnership Trade Agreement. BSA strongly supports TPP. It is essential, though, that the agreement contain the high-level obligations that are included in other recent trade agreements such as the KORUS FTA, including:

- Robust protection of technological protection measures against circumvention and against trafficking in circumvention devices;
- Protection of temporary reproductions, such as those that are made when a computer program is loaded into RAM;
- Availability, at the election of the copyright owner, of statutory damages for copyright infringement;
- Provisions granting ISPs safe harbors from liability, conditioned on implementing a notice and takedown system for hosted content; and
- Criminalization of infringements carried out as commercial activities for direct or indirect economic or commercial advantage, such as business end user piracy of software.

In addition, the TPP should adhere to the construct for permitting limitations and exceptions to copyright that is a part of Berne, TRIPs and the WIPO Copyright Treaty: complete flexibility to determine the nature and scope of exceptions at the national level, provided those exceptions meet the internationally accepted three-step test.

BSA is troubled by the Administration's July 3rd announcement of its proposal to "obligate [TPP] Parties to seek to achieve an appropriate balance in their copyright systems in providing copyright exceptions and limitations for purposes such as criticism, comment, news reporting, teaching, scholarship, and research." This appears to be an open invitation to TPP parties to establish overbroad exceptions in the name of "balance" that would be difficult to challenge. Moreover, bearing in mind that several TPP countries have software piracy rates that exceed 50%, it is difficult to see how an "appropriate balance" can be achieved by *weakening* copyright protection.

TPP should not require or encourage parties to adopt exceptions and limitations. To do so ignores the fact that all parties to the TPP negotiations already include exceptions and limitations in their copyright laws, and would give inappropriate credence to hyperbolic statements about "overprotection" of intellectual property.

Threat Assessment: Evaluation of Emerging and Future Threats

The most important emerging trend in the software industry is the growth of cloud computing. Although it is still a small part of overall information technology spending, it is the fastest-growing segment of the IT industry. By 2015, spending on cloud computing is expected to grow to \$72.9 billion, or 3.3% of total IT spending. This represents an impressive compound annual growth rate of 27.6%.

Briefly stated, cloud computing is the delivery of computing resources as a service over a network. These resources may include software, infrastructure (such as online storage or database servers) or the environment for developing and hosting Internet-based applications.

Cloud computing will profoundly change not only how software is delivered and consumed, but also how it may be stolen. For example, copying and distributing computer code without authorization becomes much more difficult in the cloud environment, where the code never leaves the cloud server. Nevertheless, piracy of cloud computing services takes place – though it is still more of an anticipated problem than an actual one. Cloud piracy is most likely to take one of two forms:

- Unauthorized use of a cloud service; and
- Offering a cloud service using software that is not licensed for that purpose.

Unauthorized use: When software is delivered as a service, the code remains on the server and is never circulated. No copies, permanent or temporary, are made on the user's computer. While streaming of music or audiovisual content constitutes a public performance, it's unclear whether the same could be said of delivery of software functionality over the Internet. Consequently, it is uncertain which, if any of the exclusive rights under copyright law apply when one uses a cloud service without authorization. This may be an area that requires legal clarification in the US and overseas.

"Dark Clouds" – Unauthorized cloud services: Not all cloud software is "born" in the cloud. Using techniques like virtual desktops, the functionality of existing desktop software can be offered through cloud services. If the desktop software is unlicensed, or not licensed for that type of use, the reproduction of the software in the cloud servers is infringing.

Although the "dark cloud" fact pattern may be somewhat novel, the legal issues are less so. From a copyright standpoint, the making of a copy of the software (in a virtual desktop in a computer server) that is not authorized by the software license is an infringement. The complexity arises from the need, in each instance, to interpret the applicable license agreement to determine what is, and what is not an authorized use.

Mobile device piracy: Piracy of mobile device-based applications ("apps") is another trend that may be on the horizon. As consumers grow increasingly comfortable using tablet and smartphone applications to perform complex tasks that – until recently – required the installation of a software client on their desktop or laptop computer, software companies will increasingly offer products that have been optimized for the mobile user experience. In some cases these offerings will take the form of application-based access to cloud services, and in such situations unauthorized use may become a concern. In some situations, third party mobile application developers may even develop applications that allow consumers to access cloud-based versions of software that has not yet been licensed by the copyright holder for such use.

Optional Questions

A. Optional Question 1: Improving Collaboration and Information Sharing to Better Address Cross-border Intellectual Property Infringement

BSA believes that the cross-border investigation of infringement may be significantly enhanced if the Administration can secure commitments from trading partners to engage in joint training programs and enforcement actions in jurisdictions where intellectual property infringement is common. Our hope is that by creating new opportunities for direct engagement between US law enforcement agents and their counterparts abroad, these joint training programs and investigations will allow all parties to achieve a greater understanding of the legal and practical impediments to successfully prosecuting intellectual property crimes in the relevant jurisdictions. Armed with a greater familiarity with foreign legal requirements and the agents tasked with enforcing them, US law enforcement entities should be able to more easily identify cases that are worth pursuing and act more quickly against infringers located abroad.

B. Optional Question 2: Fostering Greater Collaboration to Improve Efficacy of Enforcement Activities

BSA would encourage the Administration to establish an office within the Intellectual Property Rights Coordination Center that would be responsible for building relationships and acting as a primary liaison point for international law enforcement entities regarding intellectual property rights enforcement. This office could assist with running deconfliction, coordinating joint training opportunities and investigative collaboration, and could introduce representatives of US rights holders and foreign law enforcement agencies to one another upon request.

It is not uncommon for rights holders to conduct independent investigations on a global scale and avail themselves of civil remedies deemed likely to result in the successful disruption of the infringement at issue. Occasionally, individuals and/or entities targeted by rights holders' enforcement activities may concurrently be the object(s) of an ongoing law enforcement investigation in one or more countries. If a civil remedy is triggered before the relevant rights holder becomes aware of a criminal investigation, valuable data may be lost forever due to the lack of coordination. Establishing an office that is primarily responsible for facilitating IP enforcement activities that may extend beyond national borders will help reduce this risk, and will likely benefit all interested parties.

C. Optional Question 8: Detecting and Interdicting Pirate Software Delivered by Express Carrier

As noted in the Federal Register notice, the number of shipments sent through international mail and express carrier services has grown dramatically in recent years, leading to increased law enforcement efforts directed at interdicting infringing goods shipped by such means. According to the IPR Center, in FY 2011, for example, the number of seizures by mail and express consignment increased by 16% with an overall increase of 84% since 2007.

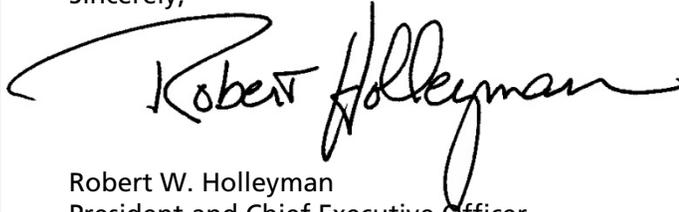
We appreciate the efforts by the Administration to convene right holders and members of the express consignment industry to improve the effectiveness of

interdiction efforts. Unfortunately there are members of the express consignment industry outside the US that do not participate in these efforts. Improved coordination with foreign governments could assist in bringing these entities to the table. Nevertheless, these discussions have identified a number of steps that could be taken to improve detection and interdiction of infringing goods, including increased coordination with right holders, simplified procedures and increased training, equipment and personnel at international mail facilities and express mail hubs.

• • •

BSA appreciates this opportunity to provide its views on the second Joint Strategic Plan.

Sincerely,

A handwritten signature in black ink that reads "Robert Holleyman". The signature is fluid and cursive, with a large, sweeping initial "R" that extends to the left.

Robert W. Holleyman
President and Chief Executive Officer