Comments of the

THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

in Response to the Request of the Intellectual Property Enforcement Coordinator For Comments on the Joint Strategic Plan

March 24, 2010

The Software & Information Industry Association ("SIIA") respectfully submits these comments in response to the request of the Intellectual Property Enforcement Coordinator (IPEC) for comment on the Joint Strategic Plan as published in the Federal Register on February 23, 2010.

SIIA is the principal trade association of the software and information industry and represents over 500 companies that develop and market software and digital content for business, education, consumers, the Internet, and entertainment. One of SIIA's primary missions is to SIIA protect the intellectual property of member companies, and advocate a legal and regulatory environment that benefits the entire industry. Consistent with these goals, for the over twenty years SIIA's Anti-Piracy Division has conducted a comprehensive, industry-wide campaign to fight software and content piracy. This pro-active campaign is premised on the notion that one must balance enforcement with education to be effective. It follows that SIIA and our members are extremely interested in the policy issues and agenda items relating to the enforcement of intellectual property rights that are raised by the IPEC in the Federal Register Notice.

PART I
ANALYSIS OF THE THREAT POSED BY INTELLECTUAL PROPERTY VIOLATIONS ON THE U.S. ECONOMY

A. THE IMPACT OF SOFTWARE AND CONTENT PRODUCTS AND SERVICES ON THE U.S. AND GLOBAL ECONOMIES

It is well established that the U.S. copyright industries contribute significantly to the U.S. economy and the Gross Domestic Product (GDP). The most recent support for this statement can be found in a study by economist Stephen E. Siwek.[1] In his study Siwek demonstrates that from 2004 through 2007, the real annual growth rates achieved by both the copyright industries were more than twice the real annual growth rates of the U.S. economy as a whole. Specifically, during 2006-2007, the copyright industries contributed 43.06% of total real U.S. growth and the value added in 2007 by the copyright industries was to $1.52 trillion, or 11.05% of the GDP. This study also shows that the total sales of copyrighted works in foreign markets increased 8% from $116 billion in 2006 to nearly $126 billion in 2007 and that the total foreign sales of copyrighted works continued to surpass those of other leading U.S. industries.

Further support for the strong contributions made by the U.S. copyright industries to the economy can also be found in a 2008 report by the United Nations Conference on Trade and Development (UNCTAD). The UNCTAD report found that from 2000 to 2005 the copyright industries achieved an "unprecedented" annual growth rate in international trade of 8.7%, with the value of total exports in creative goods and services reaching $424.4 billion in 2005.[2]

The software and information industries, in particular, have proven to be key drivers of the new economy. They are among the fastest-growing and most important industries of the U.S. and world economies. These industries publish and distribute informational content,[3] provide software applications[4] and related web-based services and create the needed infrastructure and tools to further today's software- and information-based economy. Well-known firms such as

•

[1] Stephen E. Siwek, *Copyright Industries in the U.S. Economy*, 2003-2007 Report, 2009, *available at* http://www.iipa.com/pdf/IIPASiwekReport2003-07.pdf.

[2] UNCTAD Creative Economy Report 2008, *available at* http://www.unctad.org/en/docs/ditc20082cer_en.pdf.

[3] The information industry is defined by the U.S. Government as newspaper, periodical, book and directory publishing industry, which includes businesses engaged in publishing newspapers, magazines, other periodicals, books, directories, and mailing lists, and other works, such as calendars, greeting cards, and maps. These works are characterized by the intellectual creativity required in their development and are usually protected by copyright.

[4] The software publishing industry is composed of businesses engaged in computer software publishing or publishing and reproduction. Such businesses carry out operations necessary for producing and distributing computer software such as designing, providing documentation, assisting in installation and providing support services to software purchasers.

Adobe, Symantec, McAfee, IBM, Oracle, Dow Jones, the McGraw-Hill Companies, Reed Elsevier and Thomson-Reuters, along with thousands of lesser-known companies, create products and services at the leading edge of innovation.

The software and information industries are playing the leading role in the digital revolution that is transforming all sectors of our society and of the U.S. and global economies. From financial services to healthcare and from education to entertainment, software and information technologies are improving efficiency and productivity, while providing increased customization and choice. These technologies are improving processes and value chains for businesses and other enterprises, resulting in more efficient and effective management. Individuals are empowered, gaining increased access, building community and advancing mobility.

All sectors of our society and economy are experiencing unprecedented innovation and productivity through the use of software and information. In the United States, IT was responsible for two-thirds of total factor growth in productivity between 1995 and 2002 and virtually all of the growth in labor productivity.[5] Software and information products and services are at the heart of this growth.

Revenue: The rate of growth in the software and information industries has significantly outpaced that of the U.S. economy as a whole, thus helping to sustain the expansion of the overall American economy. Revenues generated by the nation's software and information industries reached $564 billion by 2005, up by more than 10 percent since the beginning of this century.[6] When comparing the software and information industries with other major U.S. industries by revenue, the data reveals that software and information rank among the leading industries in the country.

Employment: The software and information industries generate millions of high-wage jobs, with revenue and job growth far exceeding that of the U.S. economy as a whole. The U.S. software and information industries employed more than 2.7 million Americans in 2006.[7] Net employment by these industries grew by 17 percent between 1997 and 2006, adding more than 400,000 jobs.[8]

Employees working in the nation's software and information industries are well-compensated. They earn among the highest wages in the country. The annual average wage paid in the software and information industries was $75,400 in 2006. This is 78 percent higher

•

[5] Robert D. Atkinson and Andrew S. McKay, *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution, the Information Technology and Innovation Foundation*, March 2007, p. 1 *available at* http://www.itif.org/files/digital_prosperity.pdf.

[6] Software & Information Industry Association, *Software and Information: Driving the Knowledge Economy* (January 24, 2008) at 7-8, *available at* http://www.siia.net/estore/globecon-08.pdf. (hereafter "SIIA Report")

[7] *Id*. at 8.

[8] *Id.*

than the 2006 national annual average for all private-sector workers, which was $42,400.[9] Wages in the software and information industries were higher than wages in many other major industries.

Trade: Rather than exporting from the United States, many U.S. software and information companies sell their services directly in foreign markets through their affiliates abroad. In fact, such direct sales represent a substantial share of international trade in software and information. A local presence is often advantageous because an overseas subsidiary is better positioned than the parent company located in the United States to design and distribute software and information services tailored to local market conditions and requirements. In 2004, total overseas sales (all U.S. industries) through affiliates was $483 billion. The U.S. software and information industries represented 13 percent of this total, establishing these industries as important drivers of continued U.S. economic growth.

The American software and information industries also export their products and services directly from the United States. Cross-border exports represent a smaller, but important, part of overseas trade generated by the U.S. software and information industries. These direct export sales reached almost $19 billion in 2006, representing a jump of more than 30 percent from $14.3 billion in 2000.

B. THE IMPACT OF SOFTWARE AND CONTENT PIRACY ON THE U.S. AND GLOBAL ECONOMIES, TECHNOLOGY, HEALTH AND SAFETY, AND SOCIETY

The success of the software and content industries depend on a meaningful international framework to protect the industries' intellectual property. As evidenced above, the U.S. software and content industries are among the fastest-growing and most important industries of the U.S. and world economies. However, this rapid and significant growth is threatened by the pervasive amounts of piracy and general disrespect for the rights of intellectual property owners. It threatens the livelihoods of companies that create and distribute these products and services, stifling their ability to increase investment, hire additional employees and make and distribute new and existing copyrighted works.

Copyrighted works must be protected against piracy and other unauthorized online distribution. No industry can compete with free-by-theft distribution of its own products. Online piracy threatens the legitimate commercialization of copyrighted works by driving out lawful distribution channels with access the very same, but illegal, content. There is a critical need for an effective enforcement regime that deters piracy and counterfeiting, while encouraging local investment and employment. As a direct result of the PRO IP Bill's creation of the new IPEC, there is unique opportunity to develop a national strategy that highlights the importance of innovation, creativity and respecting and protecting intellectual property.

•

[9] *Id.*

Among other things, the large-scale theft of copyrighted works undermines incentives to produce and distribute new software and information products and services. More tangibly, the Siwek report concluded that theft of copyrighted works costs the U.S. economy $58 billion in total output.[10] According to the BSA-IDC Global Software Piracy Study, 41% of the software installed in 2008 on personal computers (PCs) worldwide was obtained illegally, amounting to approximately $53 billion in global losses due to software piracy.[11] Additionally, according to Outsell Inc., informational content is illegally distributed at least 56 billion times per year, just by U.S. corporate workers alone, causing substantial monetary loses by the content industry.[12]

The economic impact of piracy does not just affect the companies that produce and distribute copyrighted works.[13] It adversely affects:

> *Consumers*. Consumers feel "taken" when they buy software, content or any other product only to find out when it arrives that it's a fake. This diminishes consumer confidence in the legitimacy of software and content purchased online. Using pirated software and content is also risky business for consumers. It increases the chances that the software will not function correctly or will fail completely and increases the user's risk of catching a debilitating virus that can destroy valuable data. Users of this illegal software often forfeit access to customer support, upgrades, technical documentation, training, and bug fixes and have no warrantee to protect themselves.
>
> *Federal State and Local Governments*. The Siwek report concluded that that theft of copyrighted works costs Federal, state and local Governments $2.6 billion in lost tax revenue.[14] They lose not only from copyright owners not paying taxes on revenue they never made because of piracy, but also to those who profit from the piracy.[15]

•

[10] *See* Siwek Report at i, 11-13.

[11] Sixth Annual BSA-IDC Annual Global Software Piracy Study, 2008 *available at* http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf.

[12] SIIA Report at .

[13] Siwek Report at p. 3 (stating the "economic impact of copyright piracy us not limited to companies that design, create and sell copyrighted works. The impact of piracy flows throughout the U.S. economy. Piracy in one segment of the economy can affect other industries because the economy is an interdependent system.")

[14] Siwek Report at i, 11-13.

[15] *See* Verne Kopytoff, *IRS urged to go after eBay sellers / Tax experts say online auctions should report users' gross sales* (February 24, 2007) *available at* http://articles.sfgate.com/2007-02-24/news/17230503_1_national-taxpayer-advocate-ebay-online-sales. (stating that "[w]hen it comes to paying income taxes, eBay's legions of small-time entrepreneurs are on an honor system in which they are supposed to declare their profits to the Internal Revenue Service. Many users, however, ignore the law or are unaware of their obligation. Now a growing chorus of tax experts is hoping to crack down on the cheating by requiring eBay -- and other online auctions, such as those on Yahoo, Ubid.com and Amazon -- to track users and report their gross sales to the federal government. Armed with such information, the IRS could better seek any taxes owed, potentially reaping millions of dollars in extra revenue for the U.S. Treasury.")

Workforce. The Siwek report concluded that that theft of copyrighted works costs the about 375,000 jobs.[16]

Businesses. Even those businesses that do not produce or distribute copyrighted products or services make revenue that directly or indirectly tied to the copyrighted works being pirated (*e.g.*, test centers that are administering copyrighted tests or the company using software to run its business). These unrelated, often small and medium sized, businesses are also adversely affected by piracy. Also, businesses that use legitimate software lose when a competitor is using illegal software or content to run its operations. It makes it that much more difficult for the legitimate business to compete with the company that is cutting corners by not purchasing licenses to software or content that it needs to operate.

In addition to the harm to the U.S. economy, piracy causes numerous other harms, such as the harms caused to:

Society. Rampant online copyright infringement contributes to a culture of lawlessness online and has created a generation that fails to respect the hard work, innovation and creativity of others. It is simply too easy to anonymously make, obtain and distribute illegal copies of copyrighted works today. Otherwise honest people who would never consider stealing a CD or book from a store have no problem stealing the digital equivalent that is illegally available online. Should this trend continue it will severely limit the growth of electronic commerce as companies may decide that it just too risky to invest in the digital distribution business models.

Connectivity. Online piracy leads to vast amounts of unlawful traffic that clogs the Internet. It slows service to legitimate users and jeopardizes the ability of broadband networks to handle increased Internet traffic. It is estimated that peer-to-peer file sharing applications represent over 20% of the total bytes that pass through the Internet and 17% of the bandwidth used during peak hours.[17] The top 1% of subscribers account for 25% of total Internet traffic, and 40% of the upstream traffic; more than 46% of top subscribers' traffic comes from file-sharing applications – which primarily contain pirated movies, music, software and content.[18]

•

[16] Siwek Report at i, 11-13.

[17] Sandvine, 2009 *Global Broadband Phenomena*, Oct. 2009 at 6, 9, *available at* http://current.com/1diai4c

[18] *Id*. at 14-15.

Mobility. Mobile applications are not immune from piracy. It is estimated that 75% of all mobile applications are pirated.[19] Many of these mobile applications are produced by small entities or recent college graduates who are trying to make a living creating and marketing their new applications. Piracy makes that a difficult, if not impossible, undertaking because unlike larger companies these creators do not have the resources to bear the brunt of piracy or to adequately protect themselves against piracy.

Some of these harms are simply not possible to precisely measure. However, this fact does not mean that the harm is not real and substantial. The impact on our economy and society is undoubtedly severe.

There are also many non-economic harms associated with software and content piracy. It is rare that we encounter a pirate who is not also engaged in some other illegal (and often dangerous) activity. Studies have also shown a nexus between piracy, organized crime and terrorism.[20] Moreover, many pirates operate sites that expose users to viruses, identity theft, malware, phishing and other types of consumer fraud or health and safety concerns. For example:

Health and Safety Issues. Health and safety issues don't just arise in counterfeit pharmaceutical or car part cases. They also arise in software and content piracy cases. Take for example, the case of Adam Perahia, a pediatrician charged with copyright infringement and child pornography. An initial investigation by the SIIA into Perahia's involvement in an electronic message board group (which provided pirated copies of medical textbooks and other copyrighted medical info) led investigators to seize Perahia's computer. One of the most dangerous examples of the pirated content were the pirated medicine dosage charts that were incorrectly and then posted with a fatal dosage amount listed. After seizing the computer, Federal authorities made an even more disturbing discovery of a cache of child pornography. Perahia was sentenced to two years in prison and five years of supervised release in July 2005.

Identity Theft. Jeremiah Mondello, formerly a college student from the University of Oregon, was sentenced by a U.S. District Court in Oregon on charges of copyright infringement, aggravated identity theft and mail fraud. Mondello received a sentence of 48 months in Federal prison, three years supervised release following jail time, and 150 hours of community service per year. Mondello's personal computers and $220,000 in cash were also seized. SIIA began investigating the eBay seller later discovered to be Mondello in 2007. Using data collected by SIIA's proprietary Auction Enforcement Tool, SIIA identified Mondello through his eBay seller ID and determined there were many more

•

[19] Garrett W. McIntyre, *Apple App Store Has Lost $450 Million To Piracy* (January 13, 2010) *available at* http://247wallst.com/2010/01/13/apple-app-store-has-lost-450-million-to-piracy/.

[20] *See* Film Piracy, Organized Crime, and Terrorism, The RAND Corporation (2009) *available at* http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf.

additional eBay identities that likely were being used by Mondello. SIIA then referred all of its case information to the Department of Justice's (DOJ) Computer Crimes and Intellectual Property Section (CCIPS) and the Department of Homeland Security's (DHS) U.S. Immigration and Customs Enforcement Cyber Crime Center -- where investigators were able to determine that Mondello was not only using a handful of falsified identities – but also created more than 40 fictitious seller IDs. He did so by recording and stealing peoples' bank account information through a keystroke logger that he distributed over the Internet. He then used that information to set up false PayPal accounts using fictitious seller names. By creating these fake seller IDs, he was able to artificially inflate his relatively high standing in the eBay marketplace, which he then used to attract sales and deliver the pirated goods.

Drugs and Weapons. Nathan Peterson, was the owner and operator of iBackups – a site that sold pirated software over the Internet, incorrectly claiming it was "backup software" (*i.e.*, legal copies of software to be used by the software licensee for backup in case of a system crash). SIIA alerted the FBI of possible software piracy by Peterson and subsequently worked with investigators and prosecutors to assure that Peterson's operation was stopped and that he was properly punished. While on bond in this case Peterson was convicted in Los Angeles for the sale of six handguns and an illegal assault weapon to an alleged heroin dealer. He was later sentenced to 87 months in prison for his copyright crimes and ordered to pay restitution of $5,402,448 and a $250,000 punitive fee.

As illustrated by these few examples, some of the largest and most damaging counterfeiting and piracy problems take place on auction sites and other commercial websites. The sale of pirated software and content on these sites is especially harmful because it not only hurts those companies that are being pirated, but it also reduces consumer confidence in the legitimacy of purchasing software and content online. Consumers may feel they are buying legitimate software and content only to find out that they have been bamboozled by an online seller who has sold them illegal products. Because these types of piracy cases involve consumers who are trying to do the right thing by buying legal product and are willing to pay money for the products, these cases of commercial piracy are especially harmful to the software and information industries as these consumers would very likely have purchased legitimate products had the illegal products not been so easily available.

Similarly, websites like Scribd, DocStoc and TESTKING are likewise havens of content piracy. These sites allow consumers to search for the content they wish to access, often allowing access to full copies of pirated books, magazines, documents, etc. While these sites may differ from the aforementioned commercial websites in that pirated works are not being sold, they still cause significant damage to content owners by allowing users to post thousands of illegal articles, reports, tests and other illegal content. Piracy of tests and testing materials is of special concern because such piracy threatens to destroy the integrity of the tests, the test takers and those administering the tests. Not to mention the impact this can have on the professions that have chosen to administer these tests to individuals as entry to a specific trade or profession.

Another significant problem of somewhat recent vintage is caused by sharehosting sites, also commonly referred to as "cyberlocker," "one-click hosting" or "file hosting" sites. These are sites, such as Rapidshare, SendSpace and MegaUpload, that provide Internet hosting services specifically designed to provide storage for files, typically, very large files such as movies, music, software, games, books, etc. Most of these sites simply provide a website address (URL) which can be given out freely to other users who can then access the file at a later point in time. Because of their ease of use and anonymity, sharehosting sites have become a haven for software and content piracy. Unlike the sites mentioned previously, these sharehosting sites do not allow for users to search for materials by name. The only way to access content stored by these websites is to have the exact URL of the file (made available initially only to the user who uploaded the content). However, there exist communities of consumers who have created "indexing" websites that archive and continually update URLs that lead to the illegal content downloads (*e.g.*, RapidLibrary.com).

Even though some of these sites are responsive to takedown notices sent pursuant to the Digital Millennium Copyright Act (DMCA) and take varying degrees of precaution to attempt to prevent piracy from occurring, the reality of the situation is that there remains rampant piracy due to users continuously uploading and re-uploading copyrighted material.

Unfortunately there are no "silver bullet" solutions to these piracy problems. There are practical limitations on the ability of copyright owners to adequately combat the problems. Copyright owners often not only lack sufficient resources to adequately combat the problem but they also often lack sufficient information about the extent and source of the piracy. Moreover, because these outlaws are continuously devising new ways to engage in piracy and to avoid detection, it is exceedingly difficult, and often impossible, for copyright owners to meaningfully combat this piracy alone. The best way to effectively address these large-scale piracy problems is through the cooperation of multiple stakeholders, including the Federal, state and local government agencies.

C. ENFORCEMENT EFFORTS BY THE SOFTWARE AND CONTENT INDUSTRIES TO COMBAT PIRACY

SIIA's membership includes a variety of businesses: software publishers, educators, test publishers, book publishers, magazine publishers, even newspaper and online content publishers. Combined, these companies continue to lose billions of dollars a year to Internet piracy. To protect its members, SIIA employs a global strategy that proactively addresses Internet piracy of SIIA's member companies' copyrighted works. Piracy has no geographical boundaries, thus SIIA monitors the Internet in multiple languages in order to protect member companies on an international scale.

Through the various initiatives conducted under its Internet Anti-Piracy Program, SIIA targets piracy of participating members' products on a wide range of Internet protocols, including websites, auction sites, classified ad sites, P2P networks, Torrent and FTP sites, sharehosting sites and other forms of electronic distribution on the Internet. SIIA monitors these protocols

using both automated and manual means and a variety of criteria, including but not limited to file size, filenames and their contextual location to generate a list of potential pirated sites.

SIIA evaluates the results gathered from its monitoring and investigations and issues DMCA takedown notices to Internet Service Providers (ISPs) (overseas ISPs receive cease-and-desist notices according to local laws) demanding that the infringing software or content be removed immediately. Where appropriate, SIIA staff will also issue cease-and-desist (C&D) letters directly to the individual(s) responsible for the piracy to prevent future infringements.

In the most egregious piracy cases SIIA will pursue civil litigation against the responsible individuals and organizations. For example, through its Anti-Piracy Litigation Program, SIIA identifies the most egregious sellers of pirated software and content on auction sites and websites (*e.g.*, eBay, Amazon.com, Craiglist, iOffer, etc.) and then sues them in Federal court demanding that they cease their infringing activities and pay a steep monetary penalty.

Through SIIA's anti-piracy efforts, we have also worked a great deal with the Office of the U.S. Trade Representative ("USTR"), Department of Justice ("DOJ"), U.S. Patent and Trademark Office ("PTO"), Department of Homeland Security ("DHS"), U.S. Postal Service ("USPS"), and other Federal and state agencies to protect SIIA member companies' copyrighted software and content.

Significantly, SIIA also pursues cases of software and content piracy taking place within an organization. This occurs when software has been installed or content is being copied and/or distributed by an organization without the proper license from the publisher.[21]

SIIA's Corporate Anti-Piracy program is driven by source reports. A person we refer to as "the Source" notifies SIIA that a particular organization is using illegal software or content (such as newspaper articles, magazine articles, newsletters, newswire services and financial reports). SIIA staff evaluate the veracity, accuracy and reliability of the source report and based on this evaluation SIIA decides whether to pursue the reported organization. SIIA pursues only those cases where there is reliable and extensive information that the reported organization has illegal copies of software or content.

If SIIA decides to pursue the organization and the affected software publisher participates in the Corporate Anti-Piracy program, SIIA will forward information about the case to them and await specific authorization to proceed against the organization. Upon receipt of specific authorization, SIIA contacts the target organization and requests that the organization conduct a cooperative investigation (such as a software audit) of all of its workstations, laptops and servers to determine the extent that software or content was copied and/or distributed illegally.

•

[21] For example corporate end-user software piracy takes place when an organization purchases a single licensed copy of a software program and installs it onto several computers, in violation of the terms of the license agreement or copies a software program onto an organization's servers where the organization's network "clients" are allowed to freely access the software in violation of the terms of the license agreement. Examples of content infringement by an organization include actions such as circulating copies of news, magazine, or newsletter articles by e-mail or hard copy (even if only internally within the company) or posting news, magazine, or newsletter articles on a website (even if they are also posted on the copyright owner's website).

After the organization conducts an investigation, it provides SIIA with the results, documenting the quantity and titles of the software and/or content it has in its possession. The organization also provides SIIA with license documentation that establishes whether it has sufficient licenses for the software or content. From here, there can be one of three outcomes:

- If unlicensed software or content is found, the organization must (among other things) delete the infringing software and content; license sufficient copies of the software and content, pay a significant fine, and adopt and implement organization-wide software and content compliance policies. In return, SIIA releases the organization from any liability it would otherwise have had under the copyright law.

- In the rare instance where no unauthorized software or content is found, the case is closed.

- If the company refuses to conduct the requested investigation, SIIA may sue the company for copyright infringement on behalf of the publishers participating in the SIIA Anti-Piracy program. SIIA considers litigation as the alternative of last resort. Nevertheless, if an organization refuses to cooperate, SIIA will - as it has done in the past - sue that organization for copyright infringement of its members' content.

SIIA prefers to settle cases amicably. In most cases, SIIA is able to reach negotiated settlements, primarily because the terms of settlement requested by SIIA are significantly less burdensome than the terms that would probably be assessed against those companies if they chose to litigate the copyright infringement claims.

PART II
RECOMMENDATIONS FOR IMPROVING THE U.S. GOVERNMENT IP ENFORCEMENT EFFORTS

Through SIIA's anti-piracy efforts, we have worked extensively with the Office of the U.S. Trade Representative (USTR), Department of Justice (DOJ), U.S. Patent and Trademark Office (PTO), Department of Homeland Security (DHS), Department of State (DOS), the U.S. Postal Service (USPS), the U.S. Copyright Office, the Federal Trade Commission (FTC), the Department of Education (DOE) and other government agencies. We have also worked closely with various state and local agencies to help us combat particular piracy problems. Over the years, these agencies have represented the interests and concerns of U.S. intellectual property rights owners -- and in particular those of SIIA and its members -- with extraordinary skill and effectiveness. The institutional intellectual property knowledge and expertise of these agencies serves U.S. industry well. In light of this, SIIA hopes that the aforementioned Federal agencies will have a significant role in formulating and addressing the agenda items and policy matters relating to the objectives in the Joint Strategic Plan.

Notwithstanding the outstanding efforts by these Federal, state and local agencies, global software and content piracy rates remain high while the number of domestic prosecutions remains relatively low. To effectively fight piracy in the United States and abroad additional resources and coordination between the agencies is necessary.

We cannot stress enough how important it is to SIIA and its members that all countries -- and most importantly, the United States -- have in place adequate and effective enforcement mechanisms for dealing with the theft of intellectual property. Without workable means for enforcing one's intellectual property rights, the rights have essentially little value. It is, therefore, imperative that barriers to enforcement not be erected -- whether bureaucratic or substantive -- and that, where appropriate, domestic and foreign governments take appropriate steps to remove existing barriers to enforcement and improve enforcement abroad.

In the international context, the standards and effectiveness of the U.S. intellectual property enforcement regime take on additional importance. As the world's leading producers of intellectual property products and services, the intellectual property laws and enforcement practices of the United States are closely monitored by our trading partners. To the extent there are barriers to enforcement in the United States that become known and exploited by our trading partners, these barriers adversely affect our ability to achieve higher standards of intellectual property protection abroad. It is therefore, imperative that the U.S. intellectual property enforcement regime be irreproachable not only to ensure effective protection of intellectual property in the United States, but also to ensure that U.S. industry is able to achieve similar protections abroad.

As requested in the Federal Register Notice, SIIA has provided a list of recommendations for ways that the U.S. Government can improve its enforcement efforts. Several of these recommendations focus on improving existing programs that are working well, while others are more ambitious undertakings. In any event, SIIA urges the U.S. Government, and more specifically the IPEC, to develop a strategic plan involving the Federal and state agencies that will result in reduced piracy for all types of copyrighted and trademarked goods.

A. EDUCATION IS A KEY COMPONENT OF ANY INTELLECTUAL PROPERTY ENFORCEMENT REGIME

Education is a key component of any intellectual property enforcement regime. It can take many different forms, such as:

1. Education and Awareness Programs

Public education and awareness programs are an essential component in the fight against intellectual property violations. Education and training activities serve as an effective deterrent against piracy. Only by through effective educational and awareness programs can the public come to fully understand the value of intellectual property and the damage that results from piracy. The public needs to understand that intangible assets protected by copyright and other

intellectual property laws are indispensable to the culture and the economy of the United States and other countries. They must also recognize that acts of piracy discourage intellectual property owners from creating new works and making copyrighted works available to the public. They need to fully understand that ultimately it is the public that is harmed by piracy.

2. Training Programs

Training of legislators, judges, and other government officials tasked with enforcement responsibilities is also an extremely important aspect of an enforcement regime. Unfortunately, while many U.S. Government agencies conduct extensive training programs and spend significant amounts of money and resources training individuals here and abroad, these initiatives could stand an improved focus and coordination that would make them significantly more effective.

For example, many enforcement training programs conducted in other countries often lack a true intellectual property component or, when they do, the person performing the training lacks the expertise required of this often complex subject matter. It is important that the training programs be taught by those who understand international intellectual property enforcement issues. By developing an organized training plan administered and taught by experts in the field, we are more likely to see beneficial intellectual property enforcement regimes emerge from these countries.

There should also be a degree of accountability for foreign training programs. In this regard, it would be helpful if the names of those foreign nationals who attend the training programs are shared with industry representatives. This should help ensure that the appropriate personnel are being trained and that the industry is able to identify those government officials who should have sufficient understanding of intellectual property issues when confronted with a piracy problem in a particular country.

To accomplish the goals outlined above it is important for the various government agencies involved in training and education to coordinate their activities. Due to limited monetary and personnel resources perhaps the best way for the government agencies to improve these training programs is through continued increased coordination and communication among the agencies.

3. Publicizing Criminal Prosecutions

Another significant educational tool is the publicity of criminal cases. One reason for industry to use the criminal copyright enforcement system is for the purpose of deterrence. However, without sufficient publicity of successful prosecutions, there is little if any deterrent effect because other individuals engaged in illicit activities do not know that their brethren are being punished for their crimes. Therefore, when the Government successfully prosecutes someone for their IP crimes it is in their best interest and the industry's is to highly publicize the case.

Often a press release will issue identifying the criminal, the crime and the penalty that was imposed. Certainly, a press release is a good first start. However, more often than not, the press release represents the first and last step in publicizing the case. In SIIA's view more can be done

to publicize the good work by the Government in locking up these criminals. For example, when taking down a website the Government agency should make sure sites are taken down at the earliest possible instant and promptly replaced by a message explaining why the site was taken down and the penalty being served by the perpetrator. In addition, when accepting a guilty plea in case involving an IP crime, the Government could require the defendant to confess his or her crime in a publicly accessible venue, such as video posted on the agency's website. Not only would the videos serve as a deterrent to would-be infringers but the videos could also be used for education in schools and training classes.

The Government can also work more closely with industry to help publicize these cases by notifying the IP owner/victim of any impending significant action (*e.g.*, a search and seizure or plea) that the Government intends to publicize, so that the IP owner can prepare to publicize the matter as well.

B. STRENGTHEN AND IMPROVE EXISTING FEDERAL ENFORCEMENT PROGRAMS THAT HAVE PROVEN TO BE EFFECTIVE

Over the past decade the Federal Government has made great strides improving the quantity and types of enforcement activities of the various agencies involved in IP enforcement. Most of these agencies now recognize the severity and significance of the piracy problem and have devoted IP staff and initiatives aimed at addressing it. Nevertheless, piracy continues to be a staggering problem plaguing intellectual property owners. Consequently, among the various recommendations we provide in this submission, we recommend that the Federal Government strengthen and improve existing Federal enforcement programs that have proven to be effective, such as:

1. Continue and Enhance the Critical Work of the Department of Justice Intellectual Property Task Force

The DOJ and the Federal Bureau of Investigation (FBI) play a significant role in the enforcement of intellectual property. These agencies not only play a vital leadership role on important issues of intellectual property policy and adjudication but represent the software and information industries' primary point of contact for raising the possibility of criminal investigations.

In 2004, the DOJ created an Intellectual Property Task Force, chaired by the Attorney General's Deputy Chief of Staff that was comprised of numerous high –level representatives from the Criminal, Civil and Antitrust Divisions, the FBI, the Office of Legal Policy, the Office of Legal Counsel, the Executive Office for U.S. Attorneys, the Office of the Solicitor General, and the Office of Legislative Affairs. The Task Force issued a report that included many recommendations relating to criminal and civil enforcement and international cooperation. In 2006, the DOJ followed up by issuing a progress report showing that most of the recommendations had been successfully implemented.

Since the initial Task Force was created every incoming Attorney General has renewed it. The Task Force has become an integral means for coordinating the DOJ's intellectual property

enforcement functions. We were pleased to see that just recently the DOJ reinstalled the Task Force with the same level of participation as before. We are hoping that the Task Force will continue its outstanding work with a focus not only on Internet enforcement, but importantly also cooperating with the states to prevent the trafficking in pirated and counterfeit physical goods.

2. Increase the Number of IP Attachés Stationed in Other Countries

The IP attachés program[22] has become an extremely useful initiative in helping intellectual property owners and other Federal Government agencies protect and enforce intellectual property rights abroad. These IP attachés, which are stationed at American embassies in India, Brazil, Thailand, the Russian Federation, Egypt, and China have also helped provide assistance on IP issues to law enforcement agencies and judges within these countries. It is our hope that the program will be expanded into other countries as well as deploying an IP attaché to the Organization for Economic Co-operation and Development (OECD).

Also, we recommend that, in countries where an IP attaché is stationed, the DOS representative at the U.S. embassy who is responsible for IP issues should coordinate with the IP attaché to develop enforcement strategies for IP enforcement in the country and should work together, along with others at DOS, as appropriate, to implement the strategy.

3. Increase Manpower and Resources Devoted to Intellectual Property Crimes

As noted above, SIIA works extensively with the various agencies to combat software and content piracy in the United States and abroad. In most cases, we work most closely with the DOJ – including the FBI and CCIPS; DHS – including ICE; and the USPS. While their work on the various criminal cases has been nothing short of excellent, the large volume of piracy and counterfeiting cases and the complexity of these cases takes an extraordinary amount of time, money and resources. We urge the Administration to provide these agencies with additional manpower and resources so they can continue their excellent work and to investigate and pursue a higher volume of IP crimes.

4. Increase Funding for State and Local Enforcement

State and local enforcement has become increasingly important in the fight against intellectual property-related crime. This is especially true with crimes involving the illegal online trafficking in pirate or counterfeit goods. For instance, SIIA works closely with state and local enforcement to pursue those who sell pirate and counterfeit software on Craigslist.

We urge state and local enforcement agencies to continue to work cooperatively with rights owners and the Federal Government, and for the Administration and Congress to support these efforts by funding the states enforcement initiatives. In this regard, we are pleased to highlight the DOJ's recent announcement that the Office of Justice Programs (OJP) would be providing grants totaling over $1.98 million to state and local enforcement agencies to fund investigation, prosecution, prevention, training, and technical assistance relating to combating intellectual

•

[22] *See* http://www.uspto.gov/ip/global/attache/index.jsp.

property crimes. The grants can be used to reimburse expenses related to performing criminal enforcement operations; to educate the public to prevent, deter, and identify criminal violations of intellectual property laws; to establish task forces exclusively to conduct investigations and forensic analyses and prosecutions; and to assist in acquiring equipment to conduct investigations and forensic analysis of evidence. While this is a good start we would like to see increased funding devoted to state and local enforcement through this program.

5. Continued US Government Policy that Ensures Accurate, Reliable and Publicly Accessible Whois Data

By way of background, "Whois Data" refers to information about the allocation of blocks of Internet Protocol (IP) addresses (the numeric addresses for all resources connected t the Internet). Access to this information is extremely important not only for enforcement against copyright piracy and trademark infringement, but also to combat other forms of misconduct carried out online. The data includes contact information on the registrant of Internet domain names, as well as data on administrative and technical contacts, and leads for identifying the entity hosting the content on World Wide Web sites associated with the domain. When such misconduct is associated with a particular IP address, Whois enables the investigator to identify the Internet service provider or other entity to which the IP address was initially assigned, and also to learn of sub-allocations to other providers, though rarely, if ever, to the end-user. Whois provides greater transparency, so that end users know more about the parties with whom they – or their children – are interacting online. In this way, publicly accessible Whois promotes the healthy growth of e-commerce, including but not limited to e-commerce in works protected by copyright.

It is essential that U.S. policy continue to make the preservation and enhancement of this vital tool a priority.[23] The investigation of virtually every case of piracy involves the use of Whois data. For example, when an investigator seeks to determine who is responsible for a website where infringing activity is taking place, a review of the Whois data for the domain name which resolves to that site is usually the first step. This data is essential not only to law enforcement, but it is also relied upon by private parties (including copyright and trademark owners), whose independent enforcement of their rights allows law enforcement to conserve scarce resources.

The U.S. Government can preserve public access to Whois in three main ways, depending on the type of domain name registration involved:

- With regard to generic Top Level Domains (gTLDs), such as .com, .net, or .info, public accessibility of Whois depends on the terms of contracts between the registrars (and registries) and the Internet Corporation for Assigned Names and Numbers (ICANN). Through its participation in the ICANN Governmental Advisory Committee, the USG should continue to advocate for reliable, accurate, and real access to Whois Data.

•

[23] U.S. enforcement policy should also recognize that the Whois Data was collected for a wide variety of purposes, including combating fraud, promoting confidence in doing business on the Internet, and enforcement of intellectual property laws by the private sector. As such, *Whois data has always been collected and made available to the public primarily for the purpose of enabling contact with the operators of online resources to which domain names resolve (with respect to domain name Whois) or with the network operators to which an IP address has been allocated or sub-allocated (in the case of IP Address Whois).* Since IP Whois address information by itself cannot identify any end-user, other than in exceptional cases, public access to such data has little if any impact on privacy or free expression concerns.

- With regard to country code Top Level Domains (ccTLDs), such as .uk, .fr, and .de, ICANN plays almost no role on Whois, the U.S. has entered into free trade agreements with several countries that set baseline standards that our trading partners pledge to maintain in the ccTLDs allocated to each country. These standards include providing public access to reliable and accurate contact information on domain name registrants. The U.S. Government must continue to seek inclusion of these provisions in future agreements, and ensure that existing commitments are fully implemented.

- With regard to the .us ccTLD, Whois policy is set by the National Telecommunication and Information Administration (NTIA) of the U.S.. Department of Commerce. NTIA should continue to ensure that existing policy regarding Whois is maintained and that information in the .us database is accurate and up-to-date.

We strongly urge that the Joint Strategy include a reaffirmation by the U.S. Government of its policy of reliable, accurate, publicly accessible and timely Whois Data. Under the Affirmation of Commitments that now embodies the U.S. Government's relationship with ICANN, a review of Whois policy is scheduled to be launched later this year. The U.S. Government should participate actively in that review to ensure that this critical enforcement tool remains available in the gTLD environment.

As the USG is well aware, ICANN is undertaking a major policy initiative to expand the number of gTLDS, possibly hundreds, indeed, thousands of new domain names. Working through the GAC and in other fora, USG should support ground rules that set a greater emphasis on the need for the new gTLD registries (directly, or through the registrars authorized to take registrations) to verify contact data submitted by registrants, and to cancel registrations that are supported by intentionally falsified contact data. The U.S. Government should also monitor closely the negotiation of new amendments to the standard Registrar Accreditation Agreement that all domain name registrars must sign with ICANN in order to be authorized to sell registrations in any gTLD. This amendment process will address a number of issues having to do with reliability of Whois data.

C. ENSURING THE FEDERAL, STATE AND LOCAL GOVERNMENT AGENCIES ACT AS GOOD CITIZENS

If the Federal, state and local governments are to be effective in IP enforcement they must first ensure that they are practicing good copyright compliance themselves. Below are some steps governments can take to ensure that they act as good citizens.

1. Federal, State and Local Governments Need to Implement Good Software and Content Compliance Practices

Federal, state and local governments should all adopt and implement good software and content compliance practices. And each agency should have proper copyright compliance programs in place to ensure that there is no end-user piracy of software and content by government agencies.

SIIA has received numerous reports over the years through its corporate enforcement program of Federal, state and local agencies that are deploying more software than they have licenses to support. Software and content compliance policies must be adopted that require these agencies to routinely audit their systems and take corrective action where necessary.

In addition to all Federal, state and local governments having good software and content compliance policies and practice, each government agency should ensure that prior to doing business with a private firm that such firm demonstrate that it has adopted and implemented good software and content compliance practices. This can be done by simply ensuring that these firm are certified as software and content compliant by a reputable body.[24]

2. Federal, State and Local Governments-Sponsored Auctions Need to Take Steps to Ensure That Only Legitimate Merchandise is Being Offered

Another area of concern is the public auction of merchandise by Federal and state government agencies.[25] It is common practice for Federal, state and local agencies (such the U.S. Marshals Service, U.S. Customs, USPS, local Police or Sheriff's Department, etc.) to sell unclaimed or seized goods at public auctions. These auctions are conducted both in person and online. On occasion, these auctions contain counterfeit or pirated merchandise.

To the extent possible, SIIA and our members attempt to take steps to prevent these agencies from selling counterfeit goods through these auctions. Our members understand the importance of recording their trademarks and copyrights with U.S. Customs and Border Protection ("CBP") in order to provide CBP with the information to target, intercept, detain, seize and forfeit shipments of counterfeit, infringing and grey market/parallel imported goods. We also train personnel that work at some of these governmental agencies on how to identify counterfeit and pirated goods in the hopes that, once trained, there will be a greater chance that the unauthorized goods will not make it to public auction.

Unfortunately, it has been our experience that the agencies conducting the auctions rarely contact SIIA or our members to determine if the merchandise they are auctioning is legitimate. This results in the Federal, state and local governments trafficking in counterfeit goods. We have had several instances where we caught a seller on a popular auction site unknowingly offering counterfeit software for sale. In the process of settling the copyright claims against these individuals we became aware that the source of the counterfeit software was a Federal agency

•

[24] For instance, for the past 15 years SIIA has been conducting the Certified Software Manager (CSM), a globally-recognized education seminar provided to keep IT specialists, legal representatives and human resource managers properly informed on software asset management procedures and programs including: understanding copyright law and license agreements; understanding the software audit process; understanding the benefits and processes of software asset management; and developing a workable corporate software policy. SIIA also teaches a Certified Content Rights Manager (CCRM), a course designed to explain the legal issues surrounding copyright law and how it affects licensing and legally disseminating content throughout organizations. This course is designed for professionals who purchase and manage copyrighted content and are responsible for ensuring it is used legally at all levels throughout their organization.

[25] *See, e.g.*, http://www.usa.gov/shopping/shopping.shtml, http://www.treas.gov/auctions/ and http://www.usps.com/auctions/.

and the sellers believed the software was legitimate because it was obtained from the U.S. Government.

There are several ways to address this problem. The easiest way is to simply adopt policies that prohibit Federal, state and local governments from selling copyrighted and trademarked software and content. If that rule is too restrictive then these agencies should be required to first contact the copyright or trademark owner to determine if the software or content they are auctioning is legitimate before being allowed to sell it. At the very least, any government agency that conducts public auctions where copyrighted or trademarked goods are sold should adopt policies that require the agency to: (i) post on their website a list of all the items up for sale at the auction along with the relevant details of the auction with enough time for the IP owner to review the list and respond, and (ii) provide IP owners with the ability to set up an automated query that alerts them whenever an auction is scheduled to take place that contains an item that includes a search term included in the IP owner's query. Of course, these policies should also provide that any copyrighted or trademarked merchandise found to be illegal should be destroyed. In addition, IP owners should also be given the opportunity to train personnel that work at these governmental agencies on how to identify counterfeit and pirated goods.

3. The Problem of State Sovereign Immunity for Intellectual Property Infringements

In 1999, the U.S. Supreme Court in the *Florida Prepaid* decisions, and the lower court decisions that have followed, created a major loophole in our laws that is threatening the effective enforcement of our intellectual property laws. Effectively, states are immune from monetary damages that are at the heart of our nation's commitment to intellectual property protection.

As a result, there is no effective deterrent to prevent states from infringing either intentionally or unintentionally copyrighted software, content and other copyrighted products. If and when state agencies and entities are discovered to be infringing, the best we can hope for is to get them to stop - but only through the costly and time-consuming effort of going to court to get an injunction. Injunctions, while appropriate in some situations, simply do not satisfy the need for effective deterrence and resolution of damages. This is having a detrimental effect on the protection afforded to copyright holders.

The impact on our members is not a constitutional abstraction. It involves real cases with meaningful financial consequences. During the six years leading up to issuance of the *Florida Prepaid* decision in 1999, SIIA identified at least 77 matters involving infringements by State entities. Of these 77 matters, approximately 50% involved State institutions of higher learning. The other 50% consisted of State hospitals, bureaus, public service commissions, and other instrumentalities.

Yet, while states are immune to damages for infringing the intellectual property rights of others, they remain free to sue private sector (both for-profit and non-profit) organizations under Federal intellectual property laws for alleged infringements of their patents, copyrights and trademarks and collect damages. States are themselves major owners of intellectual property and have benefited from Federal law and policy to achieve this result. States are increasingly seeing their

intellectual property as strategic assets and utilizing sophisticated licensing management strategies to commercialize their portfolio.

In many cases, state entities receive immunity even when the action involves commercial activity in the marketplace -- and increasingly, state agencies and state-chartered bodies are active commercial players competing with private sector service and product providers. In licensing negotiations, States and state entities do not merely play hardball because they know they cannot be sued; they, in light of sovereign immunity, will sometimes even decline to negotiate for the right to use intellectual property they concededly are using.

It is essential that State governments act as model "good citizens." One concrete step would be to implement executive level policies and procedures that lay out in clear terms that intellectual property must be used and licensed consistent with the requirements of our nation's laws and spirit of respecting the intellectual property of creators. This would include abiding by the terms of any relevant license agreements. State governments need to do more to communicate that message throughout its departments and agencies, and to individual employees.

4. Federal Government Open Access Policies

SIIA strongly supports Government policies and initiatives aimed at disseminating the results of publicly-funded research. We believe that such policies—if implemented correctly—would be consistent with the protections afforded to America's copyright owners. However, it is essential that these policies and initiatives be limited to the direct results of publicly-funded research and not extend to value-added information products and services merely because they contain the research results. The peer reviewed journals that private-sector publishers, professional societies, university presses and commercial publishers publish are examples of such value-added products, rather than examples of Government information.

The Government should not adopt policies and initiatives aimed at creating government mandates requiring that journal articles published by the private sector, and therefore are protected under U.S. and international copyright laws and treaties, be made freely available in digital form. Such a broad application would effectively run counter to the protections afforded to copyright owners of journal articles under U.S. copyright law and various international treaties. It also provides a poor example for the protection of journal articles and other copyrighted works for our trading partners.

5. Work to Avert WTO-sanctioned Retaliation Against Intellectual Property

There is a disturbing trend in WTO dispute settlement cases involving the U.S. that retaliation of intellectual property rights is the focus in the event of non-compliance. It is essential that the USG continue to work, in such circumstances, to devise acceptable alternatives that will avert WTO-sanctioned retaliation. In the event that such retaliation cannot be avoided, it is essential that it work aggressively not to impose cross-sectoral countermeasures (outside of thresholds) and reject claims of unlimited ability to suspend concessions on intellectual property rights.

D. IMPROVE COMMUNICATION AND COORDINATION BETWEEN U.S. ENFORCEMENT AGENCIES, RIGHTS HOLDERS AND FOREIGN ENFORCEMENT AGENCIES

Another area of Federal enforcement that could be improved is the communication and coordination between the various U.S. Government agencies that have responsibility for domestic and international enforcement activities. This applies not only to prosecution of domestic piracy, but also, significantly, to activities aimed at improving intellectual property enforcement regimes abroad. It has been our experience that the lack of communication between the various agencies responsible for intellectual enforcement and training efforts has been an unfortunate obstacle preventing the U.S. enforcement and training programs from reaching their true potential. We, therefore, believe that improved coordination and communication between the various U.S. Government agencies, rights holders and foreign enforcement agencies should be one of the goals -- if not the primary goal -- of the IPEC.

Accordingly, SIIA urges that the Federal Government take steps to improve governmental cooperation and coordination amongst agencies involved in intellectual property enforcement, as well as communication between rights holders and between their foreign counterparts. Some suggested ways for doing this include:

1. Creation of a Centralized Database of IP Crime Investigators

When developing a case in a particular jurisdiction for the first time it is often difficult to identify the appropriate investigator in that jurisdiction to notify about the case. It would be beneficial to have access to a centralized database of Federal, state and local investigators, as well as international investigators and agents, that we can contact when we uncover a piracy or counterfeiting case within their jurisdiction. Ideally, this database would identify these individuals by title and agency and also include their contact information and a brief summary of their experiences with IP-crime cases. The database would be especially helpful for piracy cases that we attempt to pursue with state IP enforcement agents. For foreign contacts listed in the database it would also be useful to include information on whether they have completed training in one the Federal Government's training program and, if so, some information about the type of training. This database would help us reach out directly to investigators when we become aware of a particular IP crime in a specific jurisdiction.

2. Improved Coordination with Rights Holders

Improved transparency and communication with industry should also be a goal. Often times piracy cases are referred to agency officials and the officials do not keep the referring entity apprised of the status or disposition of the case. Having some mechanism in place that enables agency officials to provide periodic updates regarding the status of cases referred to them by industry would be extremely beneficial (provided it was conducted in a manner that did not unduly impede enforcement activities). By getting periodic updates on the status of cases, copyright owners will be able to ensure that their cases are moving forward. In addition, if agency officials were to the inform industry representatives who referred piracy cases to them as

to why a particular case was declined, it might aide industry representatives in referring better cases in the future.

3. Improved International Cooperation

The improved focus and success of enforcement efforts in the United States by rights owners and the Federal and State Government has had one unfortunate byproduct. These enforcement actions have often caused the pirates to relocate their nefarious activities to locations outside the United States – often to countries that have little, if any, enforcement regime. This is one of the most critical enforcement problems facing the software and information industries. In these cases we are reliant on the ability of the U.S. Government to work with foreign governments to address the problem. Unfortunately, that rarely results in a successful prosecution.

Over the past decade we have seen dramatic improvement in the extent to which the U.S. agencies tasked with enforcement of intellectual property work with their foreign counterparts. Years ago it was virtually impossible for the U.S. Government to work cooperatively with a foreign government on an IP case. Over the years, this has changed dramatically. However, there is still a long way to go. We urge the U.S. Government to improve and broaden its partnerships with foreign governments and multilateral agencies (like Interpol) on IP-related matters, especially those involving foreign manufacturers and distributors of pirated and counterfeit goods.

E. ADDITIONAL POLICIES THE FEDERAL GOVERNEMNT SHOULD ADOPT TO FIGHT PIRACY

The recommendations outlined above predominantly suggest steps that the Federal, state and local governments can take to improve existing initiatives, communication or cooperation. There are also several additional, more ambitious steps that the Government can take to assist rights owners in effectively fighting piracy. These include:

1. Locking Down Websites and Domain Names Used By Pirates

There are several steps the Government can take with regard to domain names and websites that can help combat online piracy. First, when the Government takes action against an online pirate it ought to shut down the website immediately and replace it with a notice explaining why the website was taken down. This will serve as an educational tool to those who may access the site looking for pirated works and educate those that may have been unaware that the enterprise was illegal. In many cases this does happen, but it needs to happen in every instance.

Second, when a website is taken down as part of a criminal case and the primary purpose of the website is for making available pirated or counterfeit goods, the Government should seek an order from the court requiring registrars or registries to keep the domain name for the offending website out of circulation for at least five years.

Third, currently copyright owners can use the DMCA to take down a site offering infringing goods. However, it is fairly easy for a site to return under the same domain name but through a different ISP. There are some steps that the Federal Government can take to potentially prevent this from occurring. For example, the Federal Government could manage a centralized database of DMCA takedown notices and provide ISPs with access to this database. The ISP could automatically check this database before agreeing to host a new website. Therefore, if the pirate attempts to re-post the website using the services of a different ISP, the ISP could first automatically check the database and reject the attempt. Search engines and others could also be granted access to this database to prevent the domain name from being sold as a search term. This would help prevent a pirate's whose website has been taken down by an ISP from creating the same website under a different domain name and then trying to direct traffic to the new website through sponsored ads on search engines using the old domain name as a search term. Of course, these steps would require the voluntary cooperation of the ISPs, search engines and others.

Fourth, as noted in more detail above, it is important that the Federal Government continue to ensure that public access to Whois data is preserved. Public access to Whois data is essential to the investigation and prompt resolution of online piracy and counterfeiting. Without it would be virtually impossible for rights owners to successfully pursue these cases of online piracy and counterfeiting.

2. Involving the IRS in Piracy Cases

The saying goes that the only two things in life that are certain are death and taxes. For pirates, it seems that only one of these is true. The vast number of people making money from piracy and counterfeiting are not paying taxes on their profits. Considering that they are selling other's copyrighted works their profit are substantial to say the least. Consequently, we think there is a need for the Internal Revenue Service (IRS) to play a role in these piracy cases. For instance, there should have a designated point of contact at the IRS so that, during a civil case, when the plaintiff discovers how much the defendant profited from the piracy, that plaintiff can report this information to the IRS and the IRS can consider whether pursue the matter separately. Having said this, we are pleased to note that recently the IRS has begun to get involved in criminal IP cases.

3. Addressing the Drop Ship or "Mule" Problem

As explained in more detail above, SIIA regularly brings civil suits against those who are selling illegal software on auctions sites and related-commercial websites. Within the last year or so we have encountered a disturbing problem in the manner in which counterfeiting on these sites occurs. We refer to this problem as the Drop Ship or Mule problem. It occurs when a U.S. citizen is recruited by email or online ads to sell counterfeit software on eBay or some other online location on behalf of an individual or entity (that we refer to as the "source") that is located abroad (usually in China, Taiwan or Russia). The source desires many bona fide U.S. seller accounts to sell the counterfeit goods to U.S. consumers in a decentralized way. By doing so the source seeks to avoid a large volume of counterfeit software being sold by any one account to avoid detection himself. The U.S. citizen signs up, agrees to post the listings, and

often never sees the goods. A buyer (*i.e.*, the auction winner) sends payment to an account controlled by the source and the source "drop ships" the infringing item directly to the buyer. The U.S. seller simply receives a small royalty check for each listing that produces a sale. This is a type of fraud and counterfeiting that harms not only the rights owner and the buyer of the software but also those who sell legitimate software on the auction site and the so-called "mules" themselves. These sellers are shocked when they receive a cease and desist letter or are sued for significant damages resulting from the counterfeiting. When they inform us of the identity of the source there is usually nothing we can do because the source resides abroad, usually in a country with lax copyright enforcement.

This problem needs to be addressed through both education of the sellers, which we already do, and through enforcement, which we need the assistance of the Federal Government to do. This is not your typical IP crime as there is no way to know who the "mules" are until we proceed civilly against them and they disclose the source of the counterfeit goods and we determine that the source is the supplier in many of our civil cases. It is our hope that the Federal investigators could work with their foreign counterparts to pursue the source for criminal liability.

4. Working With Credit Card Companies to Cut Off Pirates' Money Supply

As explained above, a pervasive problem for software and content companies is the online sale of pirated and counterfeit software and content, frequently hosted in foreign countries where copyright enforcement is impracticable. The sites selling the offending software and content typically accept major credit cards as payment. These sites divert potential paying customers from legitimate resellers and may be perceived as having a patina of legitimacy deriving in part from their acceptance of credit cards.

In *Perfect 10, Inc. v. Visa International Service Ass'n,*[26] a divided panel of the Ninth Circuit held that Visa/MasterCard and several banks and data processing services were not, as a matter of law, contributorily or vicariously liable for copyright infringement by virtue of use of their cards to pay for infringing material available through various websites. However, even if copyright liability might not compel credit card companies to address piracy matters, concerns about tarnishment of their brands by association with illegal activity and their ability to recover debts incurred for illegal activity might be sufficiently compelling. This seems to be the case in other areas of illegal activity. For example, many major credit card companies appear to have programs of policing the Internet for certain violations of their rules, such as sites engaged in child pornography.[27]

•

[26] 494 F.3d 788 (9th Cir. 2007).

[27] Visa (as well as American Express) testified at congressional hearings concerning child pornography that they employed web crawling technology to monitor websites for child pornography. *See Deleting Commercial Pornography Sites from the Internet: The U.S. Financial Industry's Efforts to Combat This Problem, Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce*, 109th Cong. 71-72 (2006) (statement of Mark McCarthy, Senior Vice President, Public Policy, VISA U.S.A., Inc.) ("*McCarthy Statement*"); *Christenson Statement* at 55.

The Federal and/or State governments have been involved in many prominent successful cases which entailed enlisting the aid of credit card companies to help prevent illegal activity. We recommend that the Federal Government explore means of enlisting the support of the payment card industry and other payment processing companies for intellectual property crimes as well. Another potential option would to provide rights holders with the ability -- not unlike that provided under the notice and takedown provisions of the DMCA – to notify a credit card company or payment processing company of an instance of online piracy or counterfeiting that accepts payment using a company's credit card and request that the company terminate its relationship with the site. While not stopping the piracy, it would make it harder for pirates to profit from their activities and remove the aura of legitimacy that pirates enjoy by presenting established payment processor trademarks on their sites. If credit card companies are concerned about their liability if they terminate a merchant, similar to the DMCA, the law can provide them with indemnification for such termination.

5. Alleviate the Disincentive for Rights Owners to Bring Civil Suits Against Internet Pirates

Through its Anti-Piracy Litigation Program, SIIA regularly brings civil suits on behalf of our members against those who are pirating software and content. In many cases, the defendant pirate is found liable for significant damages caused by the IP violation. However, the pirate is often judgment proof (*i.e.*, financially insolvent and incapable of paying for the resulting damage). Frequently the pirate has long since spent the money made from the piracy and it cannot be recovered by the rights owner. To add insult to injury, not only are the rights owners harmed by the damages caused by the pirate, but in these instances they are also out additional money resulting from the significant attorneys fees and court costs that are incurred to sue the defendant.

There is often no way to know that the defendant is judgment proof before a civil case is brought by the copyright owner. In this instance the copyright owner is in a no win situation. The options are to either let the piracy continue and continue to incur damages or to sue civilly. While the infringement will eventually stop, it will cost the rights owner a significant amount in court costs and attorneys fees.[28]

Another option is to try and get the site or activity to stop by using the notice-and-takedown provisions of the DMCA or a cease-and-desist letter sent directly to the perpetrator. This approach may be effective against someone who does not realize they are engaged in piracy (like the "mule" example above), but most others will simply continue the illegal activity under a different identity or website. As a result, the DMCA notice and takedown process results in a game of "whack-a-mole" and is of limited benefit.

The last option -- convincing a Federal agency to bring a criminal case – is meaningful in only the most egregious cases. Because of the limited resources, the vast number of piracy cases, the length of time it takes to bring a criminal case, threshold requirements for cases and other

•

[28] Although the copyright law allows attorneys fees and court costs to be recovered in certain instances, if the defendant is judgment proof it will be impossible to collect them.

factors, there are practical limits to the number of potential leads we can forward to the Federal and state agencies.

If a civil case is brought against a pirate and the defendant turns out to be judgment proof, we forward the information we have about the case to a Federal or state agency and request that they bring a criminal case against the defendant so that the defendant pays some penalty for his crimes. However, these agencies are generally unwilling to take a case against a defendant once the defendant has been sued civilly by the rights owner for the same acts. The result is that rights holders and their representatives, like SIIA, spend a tremendous amount of money and resources pursuing pirates where the only sanction the pirate gets is the equivalent of a slap on the wrist.

This creates a significant disincentive for intellectual property owners to bring civil piracy cases. While larger rights owners may be able to shoulder this economic burden of enforcing their rights, small and medium sized rights owners normally cannot. Something must be done to reduce or remove this disincentive.[29]

6. Federalize Law Requiring Certain Sellers of Copyrighted and Trademarked Goods To Disclose Correct Name and Address

In addition to the lawsuits brought by SIIA under our Anti-Piracy Litigation Program, SIIA sends monthly cease-and-desist letters on a massive scale to those selling illegal software and content on auction sites and classified ad sites. The letters contain a demand informing the sellers to surrender infringing merchandise, provide relevant source information, and make a payment for all damages and costs incurred by the SIIA in connection with each infringing listing. These restitution demands are far less than the amount that may be awarded pursuant to the Copyright Act. The payment of restitution is offered as a "settlement" in lieu of litigation.

In order to send these cease-and-desist letters or to sue SIIA must obtain seller contact details from the site. However, sellers posting illegal products rarely provide these sites with accurate names or addresses. As a result, even though the sites are willing to turn over the seller's contact information, the information is often not useful. SIIA faces a significant challenge enforcing its members copyright on these sites because such false contact information severely limits SIIA's ability to pursue these egregious offenders.

To address this challenge, SIIA began to cross-check the contact information for sellers posting infringing auctions and ads by using a USPS certified web-based program. The goal was to

•

[29] While we do not propose any change in the law here, it may be worth considering different approaches, such as granting a tax credit to rights owners for any uncollected intellectual property enforcement judgments in cases where the attorneys fees and court costs in the case are greater then the amount able to be collected. The tax credit could be equal to the difference between the attorneys fees and court costs and the collected damages. Another possible approach is to give trade associations standing to bring copyright infringement actions on behalf of their members. A trade association generally has a greater ability than its small and medium-sized right owner members to devote resources and incur the monetary expenditures necessary to bring civil copyright cases. It, therefore, also has a greater ability to shoulder some of the economic burden of bringing these cases when the defendant turns out to be judgment proof. Consequently, granting associational standing for the purposes of enforcing copyright claims may to some extent help reduce the disincentive of bringing such cases.

decrease the amount of illegal software and content being sold by getting the accounts of sellers providing false information suspended. SIIA urged the sites to immediately suspend any seller providing incorrect contact information. However, the sites have been either slow or reticent to do this. Further, even where they do suspend the seller it is too easy for the seller to activate a different seller ID and sell under a new fake identity.

We recommend a Federal law be enacted that requires a person who is selling or offering for sale copyrighted or trademarked goods online through a third party for the purposes of commercial advantage or private financial gain to disclose their true name and address to that third party. [30] We believe that this would go a long way to reducing the amount of piracy and fraud on these auction sites, classified ad sites and related sites.

CONCLUSION

In closing, we would like to thank you for the opportunity to provide these comments. If you have questions regarding these comments or would like any additional information please feel free to contact Keith Kupferschmid, SIIA's Senior Vice President of Intellectual Property Policy & Enforcement, at (202) 789-4442 or Keithk@siia.net.

•

[30] A somewhat similar approach was taken by the State of California law, which passed a law making it illegal for a person to electronically disseminate a recording or audiovisual work without disclosing their true name and address. 19 Cal. Jur. 3d Criminal Law: Miscellaneous Offenses § 174, Failure to disclose origin of recording or audiovisual work. To be clear, this proposal would not require the seller to disclose their name and address to the buyer but would require them to disclose such information to the auction or related site so that rights owners would be able to locate them if we wanted to send them a cease and desist letter or sue them.