Special 301 Recommendation: Saudi Arabia should be elevated to the Priority Watch List in 2008.

EXECUTIVE SUMMARY

Saudi Arabia is generally viewed as having the worst enforcement regime and, for most copyright industries, the highest piracy levels in the Middle East. Despite its close economic ties with the U.S., the Saudi government continues to rebuff the copyright industries’ efforts to enforce their rights. In 2007, piracy losses continued to grow and the enforcement climate continued to deteriorate. IIPA recommended that the Kingdom be placed on the Priority Watch List both in the fall of 2006 in its out of cycle review submission¹ and in its full 2007 Special 301 submission in February 2007.² It has been fully two years since the Saudi government told IIPA and its members that it would (a) make its enforcement system transparent; (b) begin imposing deterrent penalties, including prison sentences, on pirates (including enforcement against corporate end users of unlicensed software); (c) ensure the systematic involvement of the police; and (d) legalize use of business software in government ministries. These commitments have simply not been fulfilled.

Industry frustration at this woeful lack of progress is at its highest point and IIPA strongly urges USTR to move the Kingdom from the Watch List to the Priority Watch List in 2008.

PRIORITY ACTIONS TO BE TAKEN IN 2008

Transparency
• The IPR Committee and the Ministry of Culture and Information (MOCI) must open up the MOCI enforcement process by having it provide full reports on the details of each case it commences following a raid to the relevant right holder(s) so that the right holder(s) (or their representatives) can follow up with appeals and related actions. Transparency, for right holders and the general public, throughout the enforcement process, including imposed sanctions, is a critical element to bringing deterrence into the Saudi enforcement system.
• Right holders must be allowed to participate in the MOCI enforcement process through directly appearing before the Breach Committee (or as it is sometimes known, the Violations Review Committee (VRC)), including seeking compensation as required by TRIPS.
• MOCI transparency will allow right holders to appeal, at their discretion, inadequate, non-deterrent sentences to the Board of Grievances.

Deterrent Enforcement
• The Governor of Riyadh, Prince Salman, should fulfill his January 2006 commitment to activate a new Special Committee on enforcement which would establish a new regime for imposing increased

penalties including imprisonment and securing the creation of a special police task force to work with the MOCI. Deterrent penalties and transparency are TRIPS requirements.

- The IPR Committee, headed by M. Al-Aiyash of the Ministry of Commerce, should work actively with industry to secure increased penalties and a more transparent process at MOCI.
- The Breach Committee (or VRC) in the MOCI must issue significant fines up to the maximum allowable in the copyright law.
- Right holders must be able, as TRIPS requires, to appeal any Breach Committee–imposed fine which is considered inadequate to the Board of Grievances, which must impose imprisonment in appropriate cases, and significantly increase fines.
- The police must become systematically involved in copyright enforcement against both street vendors and those up the supply chain (warehouses, etc.), and against corporate end-users of unauthorized software, including those initiated through a request from the MOCI, or directly by right holders. It is essential that police-led raids also result in criminal charges against copyright violations.
- A special cyber crime and IPR unit should be created by the police authorities.
- Inspections and raids on retail establishments, storage areas, distribution hubs, and duplication sites, must be sustained and enforcement run “up the chain” toward the sources of production (i.e., importers, distributors, duplication sites), including against corporate end-users of unauthorized software.
- Street vendor piracy must be completely cleaned up and offenders should be subjected to deterrent penalties, not just deportation, which has proven to be an ineffective deterrent.
- Actions against retail establishments must result in the application of criminal charges. Unfortunately, raids effected against street vendors, distribution centers and duplication sites are not resulting in criminal charges unless a retail outlet is clearly identified with that same establishment.
- Prince Salman, through the Special Committee, or through other means, must inform the management in compounds that they must pay license fees for the redistribution of TV signals and raid the compounds if they fail to comply.
- The customs system must be reformed to establish an IPR Task Force and customs officers must be provided with ex officio authority to suspend the import of pirate product into the Kingdom.
- The Communication and Information Technology Commission (CITC) must be more responsive to Internet piracy; it now only responds when pornographic materials are involved.

Ensure Legal Use of Copyrighted Materials

- The IPR Committee (and the Special Committee, if activated) must secure and implement a mandate for government ministries to fully legalize their software use, in accordance with the existing software decrees, to set an example for the private sector.
- Universities must be ordered to regulate procurement practices to ensure purchase of authorized copies of books (and other copyrighted materials), following up where necessary to ensure that those universities comply with the law.
- Tougher enforcement actions must be taken against enterprise end-users of unauthorized software.

Copyright Law Reform

- The promised internal “study” of the WIPO Internet Treaties must be completed as soon as possible and action taken to ratify and implement their obligations in the copyright law.
- Maximum penalties in the Copyright Law must be increased to deter organized criminal activity that is rife throughout the Kingdom.

For more details on Saudi Arabia’s Special 301 history, see IIPA’s “History” Appendix to this filing. Please see also previous years’ reports.

---

3 Such unit could be based on the model in place in Lebanon.
SAUDI ARABIA
Estimated Trade Losses Due to Copyright Piracy (in millions of U.S. dollars) and Levels of Piracy: 2003-2007

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Loss</td>
<td>Level</td>
<td>Loss</td>
<td>Level</td>
<td>Loss</td>
</tr>
<tr>
<td>Records &amp; Music</td>
<td>25.0</td>
<td>60%</td>
<td>20.0</td>
<td>50%</td>
<td>20.0</td>
</tr>
<tr>
<td>Business Software</td>
<td>120.0</td>
<td>51%</td>
<td>115.0</td>
<td>52%</td>
<td>105.0</td>
</tr>
<tr>
<td>Motion Pictures</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>95.0</td>
</tr>
<tr>
<td>Entertainment Software</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Books</td>
<td>NA</td>
<td>NA</td>
<td>8.0</td>
<td>NA</td>
<td>10.0</td>
</tr>
<tr>
<td>TOTALS</td>
<td>145.0</td>
<td></td>
<td>143.0</td>
<td></td>
<td>135.0</td>
</tr>
</tbody>
</table>

PIRACY AND ENFORCEMENT UPDATES IN SAUDI ARABIA

For two years now, the piracy situation has steadily worsened in Saudi Arabia across most copyright sectors active in the Kingdom. Several forms of piracy are at an all time high due to lack of deterrent penalties actually meted out (despite the maximum penalties available under the new Copyright Law) and lack of transparency. Some copyright industry groups report that the legitimate market is actually contracting, with many retail stores closing down due to high piracy rates. Industry anti-piracy efforts in 2007 continued to be substantial. Many raids, including large raids against warehouses, were run but achieved no deterrence in the market.

In 2005-6, the organization representing most U.S. right holders in the Kingdom, the Arabian Anti-Piracy Alliance (AAA), conducted a “fear factor” survey, which showed that the deterrent impact of the then current enforcement and penalty system was virtually non-existent. This resulted in increased awareness of the problem of piracy in the markets. This survey clearly demonstrated that 75% of persons in the movie retail market indicated that a pirate will never be imprisoned; 89% felt that the owner would never be imprisoned; 70% felt that the retail establishment would never be closed; and 85% felt that a pirate would never be deported.

The industry has continued to hold many meetings and engaged in many consultations with the Saudi government, but due to the intransigent attitude of the MOCI and others, no progress has been made. The President of IIPA even visited Saudi Arabia in January 2006 to address these many issues, and while promises to provide greater transparency were made at the highest levels, fully two years later, we have yet to see concrete results.

---

6 The methodology used by IIPA member associations to calculate these estimated piracy levels and losses is described in IIPA’s 2008 Special 301 submission at www.iipa.com/pdf/2008spec301methodology.pdf. For information on the history of Saudi Arabia under Special 301 review, see Appendix D at (http://www.iipa.com/pdf/2008SPEC301USTRHISTORY.pdf) and Appendix E at (http://www.iipa.com/pdf/2008SPEC301HISTORICALSUMMARY.pdf) of this submission.

7 BSA’s 2007 statistics are preliminary. They represent the U.S. software publishers’ share of software piracy losses in Saudi Arabia, and follow the methodology compiled in the Fourth Annual BSA and IDC Global Software Piracy Study (May 2007), available at http://w3.bsa.org/globalstudy/. These figures cover, in addition to business applications software, computer applications such as operating systems, consumer applications such as PC gaming, personal finance, and reference software. BSA’s 2006 piracy statistics were preliminary at the time of IIPA’s February 12, 2007 Special 301 filing and were finalized in June 2007 (see http://www.iipa.com/statistics.html) as reflected above.

8 MPAA’s trade loss estimates and piracy levels for 2006 and 2007 are not available. MPAA did provide 2005 estimates for a select group of countries, using a new methodology that analyzed both physical/"hard goods" and Internet piracy. Details regarding MPAA’s methodology for 2005 and prior years are found in Appendix B of this IIPA submission.

9 ESA’s reported dollar figures reflect the value of pirate product present in the marketplace as distinguished from definitive industry “losses.” The methodology used by the ESA is further described in Appendix B of this report.
**Optical Disc and Internet Piracy:** Optical disc piracy remains the major hard goods piracy problem in the Kingdom. Both factory produced discs (some locally made, but most imported) and “burned” discs continue to flood the markets. Street vendor piracy remains rampant throughout the Kingdom, and has gotten worse in the last year. Pirates sell pirate optical discs, including locally produced CD-Rs and DVD-Rs and imported pirate DVDs, predominately imported from the Asia Pacific Region (Malaysia, China, etc.) into commercial hubs. The Internet penetration rate in the Kingdom is growing with resulting growth in Internet piracy. Fortunately, the Kingdom’s enforcement authorities have succeeded in taking down many pirate websites, upon request of right holders, but only under its censorship regime and usually where pornographic material is also involved. IIPA urges the Kingdom’s enforcement agencies, including the Communication and Information Technology Commission (CITC), to use their authority in piracy-only cases.

**Organized Crime:** Piracy in the Kingdom has also been linked with organized crime elements in Saudi Arabia. For example, in mid-December 2007, the authorities conducted a raid against four warehouses in Riyadh. In addition to the seizure of close to 500,000 units of pirated music and video cassettes, VCDs and DVDs, the police found a large cache of explosives and weapons. Fifteen individuals were arrested.10

**Signal Theft and Piracy in the Compounds:** Signal piracy on compounds remains a very serious problem in Saudi Arabia. The compounds may have upwards of hundreds/ thousands of homes under one management/premise/security wall. Pay TV channels are usually centrally controlled and operated by the management of a given compound. The compounds utilize a smart card, installing it in their centralized head end and then redistributing Pay TV channels to thousands of homes.

Despite a continuous dialogue extending over years from the pay-TV industry and a number of raids, awareness campaigns and letters from the MOI, we still have yet to witness any significant change in the compounds. Part of the reason is that the owners of the compounds are very influential. Due to heightened security in entering compounds, affecting successful raids is next to impossible, since by the time the raid team finally gets to the head end, following delays navigating the multiple security checks, the evidence of piracy has conveniently disappeared.

IIPA itself raised the rampant theft of pay-TV signals and of audiovisual programming in the Kingdom’s compounds in its January 2006 visit and again with the Saudi delegation in September 2006. While the MOIC indicated that it can be involved in raiding such compounds, it explained that the raids must be done with the police and that police participation must be authorized by each city’s Governor’s office. In the January meeting in Riyadh, IIPA raised this issue with Prince Salman, the Governor of Riyadh. Unfortunately, industry has received no reports that raids have been conducted on these compounds since these meetings.

**Piracy of Business Software:** While the piracy rates for business software continue to be roughly constant, dollar losses to the software industry have gone up each of the last two years, due primarily to enterprise use of unlicensed software. Losses increased to $120 million in 2007 with a piracy level of 51% of the market. On the retail side, BSA, in contrast to past years, reports that the police have been receiving its complaints and in 2007 raids were run against 48 resellers and street vendors dealing in pirate or counterfeit software. Most pirate software is sold in open commercial markets but it has proved extraordinarily difficult to interest the police in these blatant, open air activities. But even this retail raiding activity has proved difficult for the business software industry.

In past years, this retail piracy was conducted primarily by non-Saudi immigrants who were then threatened with deportation when caught. This proved hardly a deterrent; there were always new

---

10 IIPA reported that early in 2005, for example, Prince Salman ordered a series of raids in the Al Batha area of Riyadh against hard core criminal activities, which unearthed many criminal operations that were involved with prostitution and narcotics. The police also encountered and seized millions of pirate DVDs, showing that piracy is providing easy funds to sustain other hard core criminal operations.
immigrants to take their place. In 2007, because the business is so lucrative and with minimal risk, BSA has seen the influx of more and more Saudi citizens involved in this illegal retail trade.

Over the years, there have been only a few raids on enterprise end users of unlicensed business software. This type of piracy causes the greatest losses to the software industry. Enforcement must be done by the MOCI which has been notoriously difficult. The Breach Committee has been extremely reluctant and has thrown up all kinds of procedural hurdles, including blaming the industry for faulty complaints (but without providing clear guidance on what they want). Many complaints from industry are rejected on formalistic grounds (e.g., power of attorney, signatures, etc.) In 2007, only 19 end user raids were run by MOCI, and often the MOCI inspectors were prevented by the raid target from entering the premises, and no further action was taken by the MOCI. If the MOCI is to be truly effective in combating end user and other forms of piracy, it must invest in increasing the number of anti-piracy inspectors to well beyond the present 10-20 full-time employees and use these resources to conduct proactive, ex officio raids.

**Book Piracy:** Saudi Arabia’s publishing market continues to experience some piracy of academic materials at certain universities. Pirate commercial offset prints as well as illegally photocopied books, especially textbooks and English language teaching (ELT) materials, continue to be available. Some universities have regulated purchase practices (i.e., they “buy centrally,” which means that all the adoptions within a university are collated by its purchasing department, which runs an on-campus bookshop). IIPA hopes to see more universities legalizing their acquisition processes by buying centrally and encourages the remaining universities to follow suit. Failing to do so invites an overrunning of the market by pirate copies, supplanting legal purchases.

**Entertainment Software Piracy:** Piracy of videogames in the Kingdom is probably the most rampant of all with pirate games available openly in retail shops in many markets as well as through street vendors. Recent hot-selling games are being imported from countries like Malaysia and are openly sold in stores and malls (whereas DVDs and music CDs tend to be made available through in-store catalogues with “runners” being dispatched off-site to obtain the selected product).

**Saudi Government Promises:** Following IIPA’s visit to the Kingdom in January 2006, King Abdullah issued a “circular” that directed that transparency and deterrent penalties should be established in the Kingdom and that government ministries should legalize their software use. Despite this clear message from the King and promises to the IIPA delegation (and further USG and industry meetings in September 2006), 2007 saw no progress whatsoever in implementing any of these reforms. To date, transparency in the administrative enforcement process at the MOCI has not been established and the Breach Committee (VRC), has failed to issue deterrent fines.

**Lack of Transparency:** IIPA members’ local representatives report that the MOI has yet to provide any right holder with information as to the results of the Breach Committee’s (VRC) administrative actions, including whether fines had been imposed and at what level, despite continuing requests for such information. At the September 2006 meetings in Washington DC, IIPA presented the delegation with a detailed list of issues that might be understood by MOI to stand in the way of offering full transparency (e.g., a list of possible information that MOI would demand from right holders as a condition to transparency). Despite indications that a response to this list would be given to the USG and IIPA before the delegation departed, the KSA government has still not (some sixteen months later) provided a response to these issues. The MOI also let it be known that it would create a web portal and place Breach Committee decisions and other information about MOI actions on this site. No word about what has happened with these promised plans has been provided either to the USG or to IIPA.

---

11 There appeared to be a further increase in the number of street vendors selling pirate videogames in areas like Olaya in Riyadh.
Under paragraph 266 of the WTO Working Party Report on Saudi Arabia’s accession, the Saudi government stated that right holders would have the opportunity to appeal any imposition of a fine by the Breach Committee to the Board of Grievances if the right holder felt that the fine was too low to act as a deterrent, as required by TRIPS. Paragraph 266 is binding on the KSA and such appeal right must be afforded under TRIPS and the KSA’s Accession commitment. Without the promised transparency in that process, however, and despite the promise made in January 2006 and the King’s circular, right holders have not been provided any information about, and have therefore been unable to appeal, any decision imposing fines.

As noted above, efforts to ascertain the MOCI’s requirements for right holders to receive such transparency have so far been unavailing. MOCI has regularly argued that any transparency for right holders must be based on the filing of formal complaints to it by right holders. Yet, for example, according to BSA, no raid has been run by the MOCI without BSA having filed a complaint, which it does on a regular basis and no information on case results or fines have ever been provided. One of the problems that contributes to the ineffectiveness of the KSA government’s enforcement system is that the MOCI rarely takes proactive (ex officio) raid action but instead waits for right holders to complain, despite open and widespread piracy in the shops and in the markets, visible to all. As described above, the openness of pirate activity has even increased in 2007.

In addition to affording transparency to right holders, the Saudi authorities, if they are to be successful in reducing piracy levels, must also publicize their actions within the country and undertake a major public relations campaign about those actions and that piracy is not only illegal, but is a criminal act, in the Kingdom.

**Lack of Deterrent Penalties:** In its February 2006 and 2007 Special 301 submissions, IIPA reported that the average fine issued by the Breach Committee (VRC) for an act of piracy was reportedly 10,000 riyals (US$2,674) and the highest fine ever imposed, apparently in only one case, a mere 50,000 riyals (US$13,368). A recent case provides a good example of the complete lack of deterrence caused by almost trivial penalties: the Breach Committee (VRC) has imposed a fine of 37,000 riyals (US$9,893) on the infringer, Video Jawarwah, after seizing a staggering 2,276,900 pirate units, one of the largest seizures ever in the Kingdom. As is evident from the size of the seizures in the cases we have reported over the years, the imposition of these paltry fines will never act as a deterrent to the levels of piracy that have become routine throughout the Kingdom.

The Saudi authorities themselves have acknowledged that no criminal case for piracy has ever proceeded or been concluded in the Kingdom. No pirate has ever served a jail term. Until this situation changes, piracy levels will remain consistently high and the KSA will continue to fail to meet its TRIPS enforcement obligations. As of February 2008, nothing has changed!

IIPA has continued to commend the Kingdom for its raiding activity. This is about the only positive element in the Saudi system, however, and must be tempered, as discussed earlier, with the reality that...
such raids are not only not self-initiated but fines are very low, without deterrence, and right holders are never officially made aware of them, except in the aggregate. Until the MOCI and the police begin to initiate actions on their own and the Breach Committee (VRC) and Board of Grievances begin to exact deterrent fines, piracy levels will continue to remain high.

Another deficiency is the low maximum fine that can be imposed by the Breach Committee (VRC). Most of the cases we have reported over the years demand penalties that exceed the Breach Committee’s jurisdictional limit/maximum fine of 100,000 riyals (US$26,738) and need, therefore, to be referred by the Breach Committee (VRC) to the Board of Grievances which has the authority to levy higher fines and to impose terms of imprisonment.\textsuperscript{17} IIPA has no report of any copyright piracy case that has ever been referred from the Breach Committee (VRC) to the Board of Grievances. If right holders were afforded the transparency that the Kingdom is obligated to provide, they could petition the Breach Committee (VRC), or the Board of Grievances, to move such cases to the Board for the imposition of penalties necessary to deter the kind of piracy reflected in these lists.

\textbf{Government Legalization of Software Use}: The software industry has estimated that the piracy rate in 2007 in government ministries was 75%. IIPA and BSA have asked that government ministries specifically budget for the purchase of legitimate software and that ministries set up software asset management (SAM) systems to monitor software use and full licensing. These two proposals must now be implemented by the government as part of meeting the King’s prescriptions against unlicensed software use in government. This should include an additional circular with a specific deadline and a requirement for each ministry to report back to the King on the results of the software audits they should conduct with SAM tools.

\section*{COPYRIGHT AND RELATED LAWS}

\textbf{Amendments to Adopt Key WIPO Internet Treaties’ Requirements and to Allow Saudi Arabia to Join the WCT and WPPT:} While virtually all the deficiencies in the Saudi Copyright Law have been remedied in the new implementing regulations adopted in 2005,\textsuperscript{18} IIPA has continually impressed upon Kingdom officials the importance of developing the legal infrastructure for electronic commerce by ratifying and fully implementing the WCT and WPPT. The initial reception to this suggestion was gratifying and industry and the U.S. government should work closely with the responsible agencies (including MOCI) to assist with advice and training. During the 2006 meetings in Washington, DC, the Saudi government representatives indicated that they had commenced a review of the WIPO Internet Treaties issues and that the next step was to seek WIPO’s advice on how best to proceed with implementing legislation. Since then we have not heard of any further progress.

\textbf{Optical Disc Legislation:} Reports are that there is at least one, and likely as many as four, known OD plants in the Kingdom. The authorities should adopt optical disc regulations to ensure that new optical disc production facilities only engage in legitimate licensed production. Saudi Arabia should join its neighbors that have adopted or are in the process of adopting a regulation to control the production of optical discs, i.e., a legislative framework to meet the challenge of optical disc piracy. Essential provisions for an effective optical disc regulatory scheme include:

\begin{itemize}
  \item The establishment of a competent licensing authority to grant licenses to optical disc production facilities as well as to deny, suspend, or revoke a license if that should become necessary. In addition, commercial CD-R/DVD-R “burning” (i.e., for the purpose of sale, distribution, or other commercial dealing) of copyrighted materials onto recordable optical discs undertaken by traditional
\end{itemize}

\footnote{Members of the Board of Grievances with whom IIPA met in January 2006 (and in meetings in Washington DC since that time) assured the IIPA delegation that if a case were brought to them, either directly by the Breach Committee or as the result of an appeal by a right holder, they would impose deterrent penalties.}

\footnote{Two deficiencies appear to remain, however. The law appears not to mandate destruction of infringing goods and does not require the award of costs and attorney’s fees as required by TRIPS. Furthermore, statutory prison sentences remain very low. MOCI Acting Minister Al-Akkas indicated a willingness to propose raising these terms in the near future.}
optical disc manufacturing plants or outside of such plants (the latter which is fast becoming a major problem) should be subject to registration to ensure that unregistered commercial conduct is punishable.

- The requirement to use SID Codes to trace pirate discs to their source of production.

- The establishment of licensee record-keeping requirements in the application process and after a license is granted, to provide governments with the means to judge whether an applicant qualifies for a license, and to provide maximum transparency after a license is granted (e.g., exemplars will be provided from each plant for every disc produced, allowing for transparent accounting of licensed production and forensic evidence should such be needed). CD-R burning registration should also entail record-keeping of orders.

- The ability to inspect plants (in addition to traditional search and seizure) and burning facilities, including nighttime inspections, to ensure that plants/facilities are engaging in legal activities.

- Government record-keeping of all plants/facilities and all actions taken with respect to them (e.g., inspections, searches).

- The establishment of adequate penalties for violations of a license (or burning without registering) including criminal penalties and possibility of plant/burning facility closure.

- Establish controls to track the export of discs, and export and import of equipment and raw materials, including the masters or stampers which are the key components for producing pre-recorded content (an automatic license is one common approach).

**MARKET ACCESS**

**Ban on Cinemas:** All public exhibition of films is prohibited by law in Saudi Arabia. Despite the fact that in October 2005, the government allowed a trial of one cinema to screen cartoons to women and children only, there appears to be no further removal of prohibition of a theatrical market in Saudi Arabia. This total ban is not only unfair and market-closing, it also opens the door wide to pirate operators who simply do not follow the law and bring in movies that the Saudi government has never had an opportunity to review for content or had any say in its distribution.

**Video Outlet License Requirements:** Video outlets must be licensed by the Ministry of Culture and Information. That Ministry has, however, demonstrated great reluctance in allowing general retail stores, such as supermarkets and toy stores, to obtain licenses. Such licensing requirements limit the ability of video distributors to reach important market segments.

**Restrictions on Home Video Distribution:** Foreign companies are prohibited from importing or distributing home video product in Saudi Arabia. Only Saudi nationals or Saudi-owned companies have this right. Such restrictions should be removed to encourage growth of the video market.