International Chamber of Commerce
The world business organization

Intellectual Property
Guidelines for Business

In Partnership with
ICC Commission on Intellectual Property

An ICC initiative
BASCAP
Business Action to Stop Counterfeiting and Piracy

ICC works to promote a balanced and sustainable system for the protection of intellectual property. It believes that intellectual property protection encourages innovation and the development of knowledge-based industries, stimulates international trade, and creates a favorable climate for foreign direct investment and technology transfer. This publication is a collaborative effort between ICC's Commission on Intellectual Property and ICC's BASCAP Initiative – Business Action to Stop Counterfeiting and Piracy.

About the ICC Commission on Intellectual Property

ICC's intellectual property policy is formulated by its Commission on Intellectual Property, which gathers over 300 business executives and private practitioners from 50 countries. The ICC Commission on Intellectual Property contributes world business views to governmental and intergovernmental debates on key intellectual property issues facing the international business community. It also works to raise awareness of intellectual property by initiatives such as its annual Roadmap on Current and Emerging IP Issues for Business and other publications. Visit ICC IP Commission on the web at: http://www.iccwbo.org/policy/ip/id3060/index.html

About BASCAP

Counterfeiting and piracy have become a global epidemic, leading to a significant drain on businesses and the global economy, jeopardizing investments in creativity and innovation, undermining recognized brands and creating consumer health and safety risks. A disorder of this magnitude undermines economic development, a sound market economy system and open international trade and investment. In response, the ICC launched Business Action to Stop Counterfeiting and Piracy (BASCAP), to connect and mobilize businesses across industries, sectors and national borders in the fight against counterfeiting and piracy; amplify the voice and views of business to governments, public and media – increasing both awareness and understanding of counterfeiting and piracy activities and the associated economic and social harm; compel government action and the allocation of resources towards strengthened intellectual property rights enforcement; and create a culture change to ensure intellectual property is respected and protected. Visit BASCAP on the web at: www.iccwbo.org/bascap

Contents

Foreword

Intellectual property (IP) has grown tremendously in its importance to companies, economies and society overall. Copyrights, trademarks and other forms of IP are vital to help companies develop and reap the deserved rewards of their own innovations, branding and creativity. Not only that, companies all over the world increasingly handle the IP of others in their day-to-day business, whether in producing products and services or in running their own operations.

The International Chamber of Commerce's (ICC's) initiative Business Action to Stop Counterfeiting and Piracy (BASCAP) has developed this set of IP Guidelines to help companies and other organisations manage both the intellectual property that they develop and the IP of others that they use in their operations. Based on practices in a wide range of industries, these Guidelines provide information on practical steps that can be taken to assess the effectiveness of an organisation's IP management policies, particularly in the area of copyright and trademark. These can help to help protect a firm's own IP more effectively, and to provide new options for improving performance and managing the risks associated with counterfeiting and piracy.

The Guidelines address IP management in all its forms within companies, from IP development to component sourcing, manufacturing, wholesaling, retailing and internal corporate use. This includes supply chain practices, relations with intermediaries and the handling of third-party IP. The main body of the Guidelines describes useful practices in a broad-based way, with specific examples and guidance. This is supplemented in the Annexes with more detail as to particular types of IP and activities.

Objectives

ICC/BASCAP offers the following Guidelines to help the business community

- understand and support the value of intellectual property (IP) as the basis of innovative, creative and economic activity that promotes business and national competitiveness,
- manage their own copyrights and trademarks more effectively,
- comply with the intellectual property laws protecting other companies' copyrights and trademarks,
- manage the business risks associated with infringement,
- prevent and deter counterfeiting and piracy, and
- develop company policies and practices to effect such compliance.

Company Policy

1. **Corporate policy.** Establish a corporate policy to conduct operations in compliance with intellectual property laws and related best practices. Implement specific policies, procedures and practices to promote compliance.
2. **Lawful use.** Acquire, use and deal in only licensed copies of copyright protected material, and genuine articles of trademark protected products, in carrying out the company's business.
3. **Protection of company IP.** Take reasonable steps to identify and protect the company's own intellectual property.
4. **Compliance.** Designate a senior director or manager whose responsibility includes overseeing and enforcing the company's IP policies.

Education and Awareness

5. **Employee policies.** Implement policies to encourage all employees and subcontractors to comply with the laws and the company's IP compliance policy.
6. **Training and awareness.** Train relevant employees and subcontractors (where appropriate) on IP compliance and company policy.

Supply, Manufacture and Distribution

7. **Supplier and customer notification.** Notify relevant suppliers and customers that the company complies with IP laws and expects them to do the same.
8. **Legitimate inputs.** Where possible, obtain IP related inputs for the business from legitimate and auditable vendors.
9. **Contractual provisions.** Document material IP related transactions, and supplier and customer relationships, accurately and in adequate detail.
10. **Supplier and customer awareness.** Obtain reliable identification and background information on IP related suppliers and customers.
11. **Required licences.** Obtain written proof of material IP rights and required licences, prior to manufacturing, shipping or offering IP based products or services.
12. **Due diligence.** Inspect documentation and materials for warning signs that infringing material may have been supplied or ordered. Make further enquiries as needed to determine the status of suspicious activity.

Security and Confidentiality

13. **Physical and network security.** Maintain physical and IT security sufficient to ensure the integrity of company records and operations, and to protect intellectual property and confidential material.
14. **Asset management.** Implement asset identification, inventory and control processes sufficient to ensure that material IP related assets are manageable and traceable.
15. **Trade-secret and confidential-information protections.** Use best efforts to protect the company's and third parties' trade secrets and other confidential material.
16. **Technological anti-piracy measures.** Respect, not interfere with, and maintain the security of technological anti-piracy measures used by rights owners with their IP based products and processes.

Compliance and Audit

17. **Recordkeeping.** Keep material IP related documentation and related materials for appropriate periods of time.
18. **Labelling.** Label completely and accurately all IP related products and packaging manufactured or supplied.
19. **Monitoring.** Periodically review the company's IP policies.
20. **Exemplars.** Supply exemplars of IP based products produced on production lines used in the company's operations to relevant rights owners, their industry anti-piracy bodies and law enforcement authorities on request.
21. **Co-operation with IP owners and public authorities.** Provide reasonable assistance to rights owners, industry anti-piracy bodies and law-enforcement authorities in their investigations of possible IP infringements.

Overview

The growing problem of counterfeiting and piracy poses a variety of risks for the business community. Counterfeiting and piracy involve infringement of the rights owner's copyright or trademark rights, which are referred to in these Guidelines as "intellectual property" or "IP".

To help companies better manage IP, ICC/BASCAP has developed these Intellectual Property Guidelines. The Guidelines provide information to businesses on practical steps they can take to assess the effectiveness of their IP management policies, to protect their own IP, and to consider new options for improving performance and managing the risks associated with counterfeiting and piracy.

Companies large and small in virtually every industry increasingly use and rely on intellectual property—the copyright, trademark, trade secrets and other intangible rights that underlie many products and services. The use of IP, whether branded products or components, copyrighted software, video or audio, images, books, news services, or a company's own or someone else's trademarks, is commonplace in every sector of business. As a result, companies increasingly find the need to put policies and procedures in place for managing their own and preventing the misuse of others' intellectual property.

In today's economy, the "intellectual capital" embodied in creative and branded content can be as important to economic growth as traditional capital, goods and services. IP protection helps to ensure the return on investment for intellectual capital necessary to produce a continuous stream of new innovation and creativity. This makes individual companies, industry sectors and national economies more competitive, fuels cultural, technological, social and economic development, and leads to overall improvements in our health and life.

The sheer volume of IP with which companies must deal is growing. Inadequate management of one's own IP can lead to lost market opportunities and displacement of legitimate sales by counterfeits. Inadequate management of the copyright or branded materials of others can result in civil or criminal claims, large compensation payments, and business disruptions and distractions.

In addition to this, there are broader business and societal risks from inadequate attention to IP management, such as injuries, health risks or other damage from counterfeit automotive parts, food or pharmaceutical products

These Intellectual Property Guidelines are designed to provide a useful guide for a wide range of businesses in different sectors to assist in assessing the effectiveness of their IP management policies.

ICC/BASCAP recognizes that IP management policies and requirements vary from industry to industry, and there is not one set of best practices applicable to all businesses. However, there are valuable lessons that can be learned from businesses in various sectors. S ome of the examples collected in these Guidelines may provide useful ideas that can be tailored for particular industries or segments of the supply chain.

They may be used directly as a basis for a company, for example, to create or improve internal company policies or employee manuals. The terms of these Guidelines can also be included in contracts between IP owners and suppliers, such as manufacturing plants.

They are also suitable for adoption as the basis of a compliance certification or an industry code of practice, whether voluntary or mandatory, in particular industry sectors.

These Guidelines are intended to be a "living document" that will evolve to respond to the challenges of new technologies and industry practices. Like the intellectual property system more generally, these Guidelines are intended as a balanced approach that respects the legitimate interests of rights owners, other stakeholders, the business community and society at large.

Objectives

ICC/BASCAP offers the following Guidelines to help the business community

- understand and support the value of intellectual property as the basis of innovative, creative and economic activity that promotes business and national competitiveness,
- manage their own copyrights and trademarks more effectively,
- comply with the intellectual property laws protecting other companies' copyrights and trademarks,
- manage the business risks associated with infringement,
- prevent and deter counterfeiting and piracy, and
- develop company policies and practices to effect such compliance.

Company Policy

1. **Corporate policy.** Establish a corporate policy to conduct operations in compliance with intellectual property laws and related best practices. Implement specific policies, procedures and practices to promote compliance.

   Guidance

   1.1. Intellectual property compliance can benefit greatly from the commitment of a company or other enterprise at the highest level of company management. This can be done, for example, through policy requirements adopted by resolution of its executive board or similar management body.

   1.2. "Intellectual property" or "IP" for purposes of these Guidelines refers to the legal protection of intangible rights in creative works and brands, in particular copyright and trademark, but also trade secrets, design rights and the like. Patent issues are more complex, and are not addressed or covered by these Guidelines.

   1.3. IP management requirements vary from industry to industry, and there is not one set of best practices applicable to all businesses. However, there are lessons that can be learned from businesses in various sectors that take the protection of IP seriously. Several existing policies warrant consideration, including for optical media manufacturing the IFPI Good Business Practices for Optical Disc Mastering & Manufacturing Plants. For the software

and information-technology industries, procurement and asset-management guidelines and standards contain useful IP compliance practices, including in the Business Software Alliance Software Management Guide, the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT®) version 4.1, and the ISO standard ISO/IEC 19770-1, Software Asset Management. Note that many of the recommendations in these ICC/BASCAP IP Guidelines can form a useful basis for a corporate policy.

2. Lawful use. Acquire, use and deal in only licensed copies of copyright protected material, and genuine articles of trademark protected products, in carrying out the company's business.

Guidance

2.1. This commitment covers the entire range of a company's input, use and output activities that involve IP related products or services. The commitment to purchase only legitimate IP based materials for use in a business or as part of a supply chain is described in more detail below.

2.2. Products used in business but not directly included in manufactured outputs, such as computer software, reference books, news services, and the like, are typically protected by copyright as well as trademark and are infringed by unlicensed copying and distribution. This commitment requires not copying or using infringing materials of this sort in the business.

2.3. IP based products manufactured or put into circulation by a business without the authorisation of the rights owner are also infringing. This includes such products as discs containing unlicensed copyright material (films, music, software, games), and fake branded goods (e.g. computer hardware, industrial products, food, cigarettes, automotive parts, consumer products and pharmaceuticals). This commitment requires not manufacturing, marketing, selling, distributing, disseminating or otherwise dealing in any such infringing items.

2.4. Adequate budget needs to be allocated for all IP related materials used in the business, so there is no incentive for employees to use infringing materials.

3. Protection of company IP. Take reasonable steps to identify and protect the company's own intellectual property.

Guidance

3.1. A company's understanding and protection of the intellectual property that it has itself developed not only helps the company to reap the benefits of its own creativity and innovation, it sets a good precedent for respecting third parties' IP.

3.2. Protection of a company's own IP may take many different forms depending on its sector and particular business. Review of trade names and symbols, and registration and proper usage of trademarks, are appropriate for many businesses. Documentation of original copyrightable works, and in some cases registration or notice of copyright, may be needed. With respect to industrial inventions, this may involve registration of design rights. Processes for renewing such rights, and paperwork and other evidence of the existence of such rights, should be carefully maintained.

3.3. There are a wide range of strategies that a company may employ to deter others from infringing its IP rights. Depending on a company's business and industry sector, these can include:

- Use of technological protections in its IP related products and processes.
- Selection of business partners that adhere to good IP management practices.
- Co-operation with enforcement authorities on the national, regional and international level.
- Co-operation among rights owners and intermediaries (including wholesalers, transporters, retailers, internet service providers (ISPs) and other on-line services) to take steps to deter infringement and the sale of counterfeited and pirated products.
- File criminal complaints or take legal actions as appropriate.
- Work with industry associations to combat various types of counterfeiting and piracy.

3.4. Customs offices typically require particular assistance with respect to a company's own IP. Registering intervention applications with Customs, and providing product information, training and prompt responses to Customs' requests for assistance, can substantially improve Customs' efforts to stop shipments of infringing items at the border.

4. Compliance. Designate a senior director or manager whose responsibility includes overseeing and enforcing the company's IP policies.

Guidance

4.1. For an enterprise to achieve IP compliance, it is usually necessary for someone within the organisation to be personally responsible and accountable for making it happen. This person needs to be sufficiently senior to have or obtain a comprehensive overview of the organisation's activities; to have the authority to develop and execute the company's IP compliance policies, procedures and practices; and to deal with infractions and complaints. A qualified senior director or manager generally would be the right level to fulfil this compliance function.

Education and Awareness

5. Employee policies. Implement policies to encourage all employees and subcontractors to comply with the laws and the company's IP compliance policy.

Guidance

5.1. As with health and safety codes and other requirements of the law, employees should be encouraged to comply with the IP laws and the company's policies, practices and procedures related to intellectual property. This could include commitments not to engage in any infringing activity on company premises or equipment or in any way related to the company operations, and to maintain the confidentiality of the trade secrets and other confidential information of the company and third parties.

5.2. IP compliance is regularly included in employees terms and conditions of employment, or as part of a policies and procedures handbook that is distributed to and binding on employees. IP compliance requirements are different and additional to any provisions in employee contracts or handbooks that govern IP ownership in the case of employee-created works.

5.3. Similar requirements and terms and conditions could also be included in written contracts with independent contractors.

5.4. Employees' and contractors' commitment to respect intellectual property typically should extend not only to activities carried out in the course of their direct work for the company—such as in purchasing, product development, manufacturing, marketing and the like—but also more generally with respect to their activities on company premises and company equipment. Many companies protect against the risk of unauthorized activities in this area by not allowing employees to install or use infringing copies of software, music, published materials or games on company computers, or to open the company computer network to outsiders for illegal access, transmission or storage of copyright or trade-secret material.

6. Training and awareness. Train relevant employees and subcontractors (where appropriate) on IP compliance and company policy.

Guidance

6.1. Training of relevant personnel usefully could cover applicable IP laws, licensing requirements, IP owners in the business, and the company's policies, procedures and practices.

6.2. A compliance officer needs to understand intellectual property laws as well as the business and licensing practices in the IP fields relevant to the company's business, in order to design and maintain IP compliance policies, procedures and practices that are effective, efficient and workable for the company. For example, a compliance officer in a CD replication business would typically be familiar with copyright rules related to music, licence agreements used by record companies and other rights owners, and information on the rights owners in the relevant field, such as through one of the many available public databases.

6.3. Employees and contractors likewise need IP related training and information relevant to their work. For example, a production manager in a replication plant needs to understand that it is an infringement for commercial software, music or films to be pressed onto CDs or DVDs if a licence agreement is not in place with the rights owner. In many companies, the purchasing manager needs to understand that use of a recognized brand label on a fake product is an illegal counterfeit.

6.4. It may be appropriate for the compliance officer and relevant employees and consultants to receive such training both when they take on a particular IP related role, and periodically thereafter, given employee and product turnover as well as evolution in the licensing and business practices in every field. Relevant industry professional groups as well as law firms and societies offer such training in most countries.

Supply, Manufacture and Distribution

7. Supplier and customer notification. Notify relevant suppliers and customers that the company complies with IP laws and expects them to do the same.

Guidance

7.1. One way to enhance compliance by suppliers and customers is to notify relevant suppliers and customers that the company respects intellectual property, maintains IP compliance policies,

practices and procedures, and expects such suppliers and customers to do the same, The precise obligations can be negotiated and included in the relevant contract, of course, or in separate mailings or website notices. This sets the right expectations for business dealings and can pre-empt problematic requests or activities, such as orders for supply of counterfeit products.

7.2. The company's contracts with suppliers and customers might also include provisions allocating responsibility for counterfeit goods or other IP violations. These can include IP indemnities, "make good" and financial remedies, delisting the infringer as an approved source or customer, and contract termination. These are ways in which a company can manage the IP risks in the event its suppliers or customers engage in IP infringement without the company's knowledge, consent or other involvement.

8. Legitimate inputs. Where possible, obtain IP related inputs for the business from legitimate and auditable vendors.

Guidance

8.1. Input activities such as purchasing of components or supplies, or third-party design, development, manufacturing or other services, often involve copyrighted or trademarked articles. A company can often negotiate commitments from vendors to purchase products and services that do not infringe IP laws.

8.2. Particularly for manufacturing operations, it is helpful for a company to obtain inputs only from fully auditable vendors that source exclusively from original manufacturers, franchised distributors or first owners of the goods.

8.3. More detailed "best practices" on securing legitimate inputs and other supply chain issues can be found in specific industry guides, as well as in the US Chamber of Commerce publication, No Trade in Fakes: Supply Chain Tool Kit.

9. Contractual provisions. Document material IP related transactions, and supplier and customer relationships, accurately and in adequate detail.

Guidance

9.1. One of the warning signs of a business that is at serious risk from inattention to IP issues, or that is actively engaged in counterfeiting or other infringing activity, is inadequate or missing written records. It is particularly important for companies engaged in manufacturing IP based products that their activities be properly documented and auditable.

9.2. What recordkeeping is appropriate will vary by industry and activity, but should include documentation of "material" activities with respect to IP based goods and services. This may encompass detailed and accurate written licence or manufacturing agreements, purchase and sales orders, production records, invoices and shipment documents. Records of material activities need to be sufficiently specific to identify the IP based material itself (for example, the individual industrial or consumer product unit, musical track, software or film title, drug or chemical product, food product, or trademark), quantity, price or licence fee, and correct destination and consignee.

9.3. For some sectors, it is important to keep and store master production copies and production samples securely, as they can be a protection for the company and its suppliers and customers as well as the IP owner. Particularly in the case of a dispute or claimed infringement, master copies and production samples can be helpful for tracing the source of illicit products or parts and assigning liability to the correct party.

9.4. Material transfers and licences of intellectual property rights should be in writing. This is particularly important if a company outsources development of IP related material, as many countries' laws presume that such transfers and licences are not valid unless in writing. Written agreements can prevent disputes over IP ownership and possible claims of infringement.

9.5. IP related contracts should be clear and cover all the relevant topics in sufficient detail to avoid confusion and later problems. These contracts typically include the technology or material to be used, the rights licensed or reserved, consumer or trade terms and conditions as appropriate, confidentiality obligations, monitoring and due-diligence obligations, and termination and other remedies in case of an IP violation.

10. Supplier and customer awareness. Obtain reliable identification and background information on IP related suppliers and customers.

Guidance

10.1. Much of the trade in counterfeits takes place between and on behalf of inadequately identified or anonymous suppliers and customers. Pseudonyms, post office boxes, mere "points of contact" and unidentified email addresses can be indicators of a supplier or customer dealing in counterfeits, as can the person's or company's lack of an obvious or documented connection with the industry sector for the particular IP related products.

10.2. Reliable identification and background information includes correct names, and complete addresses and telephone numbers. Brokers also should obtain and be able to provide this information in respect of the ultimate clients.

10.3. "Know your customer and supplier" is simply good business practice. Documentation of the true identity, background and contact details of suppliers and customers is not only a substantial deterrent to counterfeiting and piracy, it helps a company manage other kinds of risks, including supply, payment, quality and similar problems.

11. Required licences. Obtain written proof of material IP rights and required licences, prior to manufacturing, shipping or offering IP based products or services.

Guidance

11.1. Unauthorized copying, distribution, transmission or other dealing in copyright- and trademark-protected goods or services in the course of a business is virtually always infringement absent a licence from all of the relevant IP rights owners.

11.2. Licences should be authentic documents and typically specify each protected work or trademark licensed, the time period during which the licence is valid, and the specific uses and quantities licensed.

11.3. Needed licences should be in writing. Genuine copyright and trademark licences rarely cover an IP owner's entire range of products, trademarks or rights, or are of unlimited duration. Companies should insist that licences for duplication, manufacturing, or distribution of IP related products are very specific as to what has been licensed, for what period and for what uses.

12. Due diligence. Inspect documentation and materials for warning signs that infringing material may have been supplied or ordered. Make further enquiries as needed to determine the status of suspicious activity.

Guidance

12.1. Ignorance typically is no excuse for counterfeiting and piracy. Many IP infringements are "strict liability" violations, such as reproducing and distributing copyright material or trademark branded goods without a licence, regardless whether the material has been ordered by a customer. Due diligence on licences, goods, masters, orders, information and other items supplied in relation to IP related goods or services can reduce the risk of infringement.

12.2. Supplier and customer information, licences, goods received, production masters and order terms can contain warning signs that infringing material may have been supplied or ordered; an effective regular or spot inspection programme can help turn up such warning signs. If warning signs are discovered, further enquiries may be needed, including consultation with the relevant rights owner or industry anti-piracy body, to determine the status of suspicious activity.

12.3. Warning signs vary by industry. These may include, for example, orders for large quantities of unmarked copies of recognized products; use of well-known trademarks or claims of licence by unknown companies; large cash payments; poor-quality workmanship or packaging; removal, re-creation or separate shipment of trademark labels or technological protections; or incorrect or inadequate labelling of contents, geographic origin or production plant.

12.4. Some rights owners themselves offer information and assistance to help determine whether products or licences are legitimate; others do so through their industry anti-piracy body. Customer and supplier agreements should explicitly allow consultation with the relevant rights owner or industry anti-piracy body if there is a reasonable suspicion of infringement.

Security and Confidentiality

13. Physical and network security. Maintain physical and IT security sufficient to ensure the integrity of company records and operations, and to protect intellectual property and confidential material.

Guidance

13.1. Companies involved in manufacturing and distributing IP based goods are well served if their premises are secure and their personnel procedures are adequate to prevent theft, unauthorized access, "third shifts" or other unauthorized manufacture or shipment, disclosure of trade secrets, and other unlawful practices.

13.2. Companies involved in using licensed intellectual property often need to be able to prove and account for licensed activity. This requires secure storage of material IP related contracts, licences, financial records and other documentation—a good business practice in all events.

13.3. Copies of IP based products, trade secrets and other confidential information, and company records increasingly are held on computers and computer networks. Good information-technology (IT) security can help to keep such items secure, and to prevent IP infringement in the form of unauthorized electronic access, storage, copying, posting, transmission or disclosure of third parties' intellectual property.

13.4. Good IT security also typically includes such protections as anti-virus and anti-spyware software, internal computer and network access restrictions, firewalls and other restrictions of access from the internet to the company's computers and networks (including via peer-to-peer systems), and prohibitions on unapproved installation or distribution of IP protected material on company computers or networks. For further information on IT security issues related to IP infringement, see the IFPI/MPAA/IVF publication *Copyright and Security Guide for Companies and Governments.*

14. Asset management. Implement asset identification, inventory and control processes sufficient to ensure that material IP related assets are manageable and traceable.

Guidance

14.1. It is good practice for IP related products that a business uses in conducting its own operations, such as software and other IT products, to be inventoried and managed like other key assets throughout their life cycle.

15. Trade-secret and confidential-information protections. Use best efforts to protect the company's and third parties' trade secrets and other confidential material.

Guidance

15.1. Companies involved in manufacturing or dealing in IP based products or services often require or have access to trade secrets or confidential information of the IP owner in the course of such activities. Access to such trade secrets or confidential information typically depends on contractual or other legal obligations to use best efforts to protect and not to disclose or use the IP owner's trade secrets or other confidential information, except as expressly authorized by the rights owner. Such restrictions ordinarily would not apply, however, to the extent that such material has been disclosed by the rights owner or with its permission without such restrictions, or that a government or court order has required such disclosure.

15.2. More generally, it is helpful for confidentiality undertakings with customers and suppliers to be drafted so as to permit legitimate consultation of law enforcement authorities, or relevant anti-piracy bodies or rights owners, in the case of a reasonable suspicion of IP infringement such as in the case of a customer order for an apparently counterfeit product.

16. Technological anti-piracy measures. Respect, not interfere with, and maintain the security of technological anti-piracy measures used by rights owners with their IP based products and processes.

Guidance

16.1. IP rights owners increasingly rely on various types of technological anti-piracy measures in their products, product packaging and distribution systems, in order to prevent and deter counterfeiting. Companies involved in manufacturing, marketing and distributing such IP based products should support these goals by following any instructions from the IP owners as to how these technological protections should be applied, and not removing, circumventing, disabling or taking any other action that impairs their effectiveness in any way.

16.2. Licensed IP based products used in a company's internal business operations also may contain technological anti-piracy measures, which also should be respected. Indeed, modern copyright laws typically make it an offence to circumvent such measures.

Compliance and Audit

17. Recordkeeping. Keep material IP related documentation and related materials for appropriate periods of time.

Guidance

17.1. Good business recordkeeping is required by virtually every accounting standard and tax authority world-wide. Material IP related records and materials should be kept with other business records for a similar time period as such other records, which typically is not less than three years after their expiration (this period is longer in some countries). The records and materials to be maintained should include copies of material IP related agreements, purchase orders, production records, shipment documents, licences, masters and production samples.

18. Labelling. Label completely and accurately all IP related products and packaging manufactured or supplied.

Guidance

18.1. A common tell-tale sign of counterfeit articles is mislabelling. Articles, packaging or shipping boxes may indicate the wrong contents, or may have no labelling at all. The geographic origin or manufacturer identification on such materials may be missing or incorrect. Content listings of mixed shipments may fail to mention counterfeit articles that have been included with other items.

18.2. Although requirements may vary by industry, the labelling for IP related products manufactured, distributed or shipped should be complete and accurate as to specific products, quantities and origin. This should include applicable identification markings or codes, whether industry-standard or rights-owner specific, as to manufacturing plant, product identification, batch number and other designations.

18.3. Individual rights owners may have their own specific labelling requirements. There are also standard labelling requirements applicable in particular industries, for example the IFPI/Philips Source Identification (SID) disc and mould codes applicable to manufacturing of all optical discs. It is best practice for everyone in the supply chain to follow the applicable rights-owner and industry-standard labelling practices scrupulously and without exception.

19. Monitoring. Periodically review the company's IP policies.

Guidance

19.1. Ongoing monitoring, correction of problems, and refinement of a company's IP compliance policy, are an important part of ensuring that the company's policies, procedures and practices are workable and are followed.

20. Exemplars. Supply exemplars of IP based products produced on production lines used in the company's operations to relevant rights owners, their industry anti-piracy bodies and law enforcement authorities on request.

Guidance

20.1. Legitimate manufacturing plants should have nothing to hide. Providing exemplars, such as sample discs from each of an optical-disc replication plant's production lines, helps both to discourage counterfeiting and to track down infringers when piracy does take place.

21. Co-operation with IP owners and public authorities. Provide reasonable assistance to rights owners, industry anti-piracy bodies and law-enforcement authorities in their investigations of possible IP infringements.

Guidance

21.1. Companies dealing in IP related products and services are well served to co-operate when problems of infringement arise, such as by producing IP licences and other information relating to suspect articles, orders or activity. The fight against the black economy of counterfeit and pirate goods requires diligence and co-operation among IP owners, public authorities and companies in every part of the supply chain.

FAQs – Frequently Asked Questions

Q. What are the "ICC/BASCAP Intellectual Property Guidelines for Business"?

A. Business Action to Stop Counterfeiting and Piracy (BASCAP), an initiative of the International Chamber of Commerce (ICC), has developed this set of IP Guidelines to provide information to businesses on practical steps they can take to assess the effectiveness of their IP management policies, particularly in the area of copyright and trademark; to help protect their own IP; and to consider new options for improving performance and managing the risks associated with counterfeiting and piracy. The Guidelines address internal IP use, supply chain practices, relations with intermediaries, and the handling of third-party IP. They deal with IP management in all its forms within companies, from IP development to component sourcing, manufacturing, wholesaling, retailing and internal corporate use.

Q. Why is BASCAP doing this?

A. BASCAP developed these Guidelines to help companies of all sizes reduce the risks of intellectual property theft, and to deter piracy and counterfeiting. Piracy and counterfeiting are an economic blight with serious and disruptive consequences for companies found to be engaged in such activity. This is because piracy and counter¬feiting have broader consequences: They deter inventiveness and creativity, deprive governments of tax revenue, compete unjustly with legitimate economic activities and jobs, weaken consumer confidence in legitimate branded products, pose serious health and safety risks, and feed organized crime. Business and government together, each playing its part, can reduce intellectual property theft and the business and social damage that it causes.

Q. Why are these Guidelines needed?

A. There is a lot that companies can do to protect their own creativity and innovation in IP based products and services, as well as to reduce the risks of infringement of other companies' IP rights. The global economic trend is to increase investment in and reliance on intellectual property as an essential element of economic growth. The problem is that intellectual property is an intangible asset that requires not only legal protection but also good management and use in order to realize its full potential. These Guidelines are designed to raise awareness and provide useful information to companies as to how to manage intellectual property.

Q. Who will use them?

A. Companies large and small in virtually every industry increasingly use and rely on intellectual property, and thus can benefit from implementing good IP management policies inspired by the Guidelines. Small and medium enterprises (SMEs) and large companies involved in the development, manufacture, supply, or distribution of IP based products and services, as well as the large number of other commercial concerns that use some form of IP based material in their own business, will benefit.

Q. Is it a mandatory programme?

A. These IP Guidelines are made available as a voluntary guide that businesses can use directly or can draw upon to create or improve company policies, internal procedures or employee manual provisions dealing with intellectual property.

As a reference guide, the terms of these Guidelines can also be included or referenced in contracts between IP owners and suppliers, such as manufacturing plants. They are also suitable for adoption as the basis of a compliance certification or an industry code of practice, whether voluntary or mandatory, in particular industry sectors.

The Guidelines are designed to be useful to a wide range of businesses in different sectors, and are suitable to be tailored to deal more specifically with particular industries or segments of the supply chain.

Q. How were the Guidelines developed?

A. The Guidelines were developed after a survey and review of practices and precedents in various IP related business sectors, and represent examples of the range of elements that companies in a variety of industries are using to improve their management policies in this area. Included in this survey were the following sources, many of which are cited in the "guidance" sections of the various Guidelines:

- Individual industry guides (the film and music industries' *Copyright Use and Security Guide* and *Good Business Practices for Optical Disc Manufacturing*; and the software industry's COBIT and ISO standards for IT and software management).
- The US Coalition Against Counterfeiting and Piracy's *Supply Chain Tool Kit.*

Q. How will they be communicated and rolled out?

A. ICC is working with its national committees and member companies to share these Guidelines with industry groups and companies world-wide. ICC is making available the Guidelines on its heavily visited BASCAP website (www.iccwbo.org/bascap), and also is working with governments to promote awareness of the need for good IP management practices as described in the Guidelines.

Q. Why ICC?

A. The mandate of the ICC is to present a unified voice for world business, championing the global economy as a force for economic growth, job creation, and prosperity. Since 1919, ICC has worked to create an international market economy based on sound international trade and investment rules. This work includes establishing business codes, rules and model contracts that are used by business worldwide. To date, these have covered a wide variety of areas including international commercial terms, banking rules, and corporate governance, and now have been extended to awareness and assistance in the area of corporate IP management.

How Can I Get Involved?

1. **Review your company's IP management practices.** The Guidelines provide a useful set of ideas and tools for assessing the effectiveness of your own company's policies, procedures, practices and agreements related to IP management, particularly in the areas of copyright and trademark, and for considering new options for improving performance and managing the risks associated with counterfeiting and piracy.

2. **Communicate your own IP management policies** to your suppliers, customers and other third parties. You might wish to do so on your website, via email or in your contracts with them. If you prefer, ICC/BASCAP approves and would encourage you to put a link to these Guidelines directly on your own website.

3. **Publicize the Guidelines** among business and industry groups. You may want to encourage your own or related industry groups to disseminate or endorse the Guidelines themselves.

4. **Let your government know** that the Guidelines provide useful information to help companies manage intellectual property, which the government may want to promote. Let government know that business is doing its part in combatting piracy and counterfeiting.

Annex 1:
G8 Guidelines for Governments Use of Software in Compliance with Intellectual Property Rights

Overview

Business Action to Stop Counterfeiting and Piracy (BASCAP), an initiative of the International Chamber of Commerce (ICC), has developed a set of Intellectual Property (IP) Guidelines to provide information on practical steps that businesses and other entities can take to manage copyrighted, trademarked and other IP-protected goods and services effectively within their organisations.

Among the users of IP-based products and services are governments—and they have an interest in and responsibility for developing effective policies for managing the IP-based products and services that they procure and use. Demonstrating its leadership in this area, the G8 has highlighted particular ways in which governments can manage the use of one important IP-based product—software—to comply with IP rules.

The kinds of IP-management policies endorsed by the G8 are explained and illustrated in some detail here, with helpful examples from the main body of the ICC/BASCAP IP Guidelines and other industry and government best practices.

> *"Effective promotion and protection of IPR are critical to the development of creative products, technologies and economies.... We reaffirm our commitment on government use of software in full compliance with the relevant international agreements and call on other countries to follow our commitment."*
>
> **G8 Declaration, 8 July 2008**
>
> http://www.mofa.go.jp/policy/economy/summit/2008/doc/doc080714__en.html

The G8 Guidelines for Government Use of Software merit review by governments at every level, and it is our hope that this Annex can be a valuable source of information and further guidance for governments in the G8 and worldwide.

The G8 Declarations and Guidelines

The Group of Eight countries (G8), comprised of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom and the United States, have emphasized repeatedly the value of intellectual property for economic growth, innovation, creativity and other societal benefits.

The G8 ministers made specific declarations in 2000 and 2008 that it is important that governments' own internal use of software—a significant intellectual-property based innovation—should comply fully with intellectual property rights. In their 2009 declaration, the G8 ministers welcomed a report of their intellectual property experts' group, which among other things includes Guidelines for Governments Use of Software in Compliance with Intellectual Property Rights. (The relevant provisions of the G8 ministers' declarations and the G8 IP expert group's report are set forth in the Appendix.)

These G8 Guidelines cover at a high level the types of policies, regulations and laws that governments need to have in place "to reduce the risk that public computing resources are used to infringe IP rights, [to] set an example for the private sector and for IT users in the fight against counterfeiting and piracy, and, at the same time, safeguard the interests of security and transparency of their own administrations." The G8 Guidelines cover the areas of software use policies, security, information and awareness, and public-private co-operation.

The G8 Guidelines for Government Use of Software merit review by governments at every level. The G8 Guidelines, as well as the specific examples of how to implement such policies found in the ICC/BASCAP IP Guidelines and various industry and government best practices, provide practical ways for governments to assess the effectiveness of their IP management policies, and to manage the risks associated with counterfeiting and piracy more effectively.

1. Software Use Policies

G8 Guideline: Software Products. Governments shall not violate Intellectual Property rights in the acquisition and deployment of software, ad will establish the necessary measures to ensure the fulfilment of this commitment. The competent authorities should take measures to verify that computers employed by public administrations be exclusively provided with legitimate software.

Commentary and examples

1.1 Good internal management of software and other intellectual-property based products, components and services never happens accidentally, but is typically the product of specific directives and ongoing programmes to carry out such management effectively. The ICC/BASCAP IP Guidelines describe several helpful elements of such requirements that can be useful to government agencies, including:

- Specific policies, procedures and practices to conduct operations in compliance with IP.
- Adequate procurement policies and budgeting for IP-related materials.
- Designation of a senior director or manager whose responsibility includes overseeing and enforcing such IP policies.
- Effective supplier notification and awareness, contractual and licensing practices, due diligence, and other policies to ensure supply chain integrity.

1.2 International Standardisation Organisation (ISO) and other industry models can provide further guidance and examples for developing effective government policies to manage the use of software and other IP-based products and services. Helpful guidance includes:

- ISO standard ISO/IEC 19770-1, Software Asset Management, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33908.
- Business Software Alliance, Government Guide to Software Management, http://www.bsa.org/~/media/C72B329D6F7E4B46A7467DE0151210A1.ashx.
- IT Governance Institute, Control Objectives for Information and Related Technology (COBIT®) version 4.1, http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981.

1.3 The options for implementing this G8 Guideline are numerous and varied. Useful models include:

1.3.1 Some governments at the national, regional or local level issue ministerial or other decrees requiring government employees to procure and use only legitimate copies of software or IP-based materials and services generally.

1.3.2 Some governments implement terms and conditions of employment specifically requiring the same.

1.3.3 Some governments develop detailed procurement regulations and government contract terms specifying the requirement of legitimate supply of software and other IP-based materials.

2. Security

G8 Guideline: Use of Government Computer Networks. The competent authorities should establish the necessary measures to ensure that the use of government computer networks, including, for example, those operated by contractors, does not violate Intellectual Property rights.

Commentary and examples

2.1 As the G8 Guidelines describe, governments' computers and networks require proper security and management to protect against intentional or inadvertent misuse of all kinds of intellectual-property based material including software.

2.2 Several types of security measures are useful in this regard, which not only can help protect against IP misuse but also against broader damage to a government's systems and information. These are described in more detail in the ICC/BASCAP IP Guidelines and include:

- Physical as well as network security to ensure the integrity of the government's records and operations, and to protect confidential as well as IP-related material.
- Asset identification, inventory and control processes sufficient to ensure that material IP related assets are manageable and traceable.

- Physical, network and organisational protection of trade-secret and confidential materials.
- Maintenance of the integrity of technological anti-piracy measures used by rights owners.

3. Training and Awareness

G8 Guideline: Information and Awareness. Public administrations should undertake campaigns and/or informational initiatives to raise employees' awareness about the importance of Intellectual Property rights for innovation and the development of new products, with a view to encouraging the appropriate use of Information Technology. Public employees should be informed about network operating rules and procedures and the consequences of the illegal or improper use of public computer systems.

Commentary and examples

3.1. Employee and even contractor awareness of the reasons why protecting intellectual property is important, along with understanding what they can do in their particular role to maintain IP protection, are vital components of a government's effective management of software and other IP-protected materials.

3.2. The ICC/BASCAP IP Guidelines elaborate several ways in which it may be appropriate to train employees and relevant contractors:

- Training to cover applicable IP laws, licensing requirements, IP owners, and the government's laws, policies, procedures and practices related to IP.
- Detailed training for compliance officers.
- Relevant training for others depending on their role, e.g. ordinary user, IT professional, procurement personnel.
- Initial training as appropriate, for example when an employee starts work or takes on a new role related to IP; periodic training thereafter, given employee and product turnover as well as evolution in IP licensing and business practices. Note that relevant industry professional groups as well as law firms and societies can offer such training in most countries.

4. Co-operation with IP Owners

G8 Guideline: Public-Private Sector Collaboration. Aware of the crucial importance of public procurement in fostering innovation in the software industry, governments may collaborate with the private sector and other stakeholders to share best practices related to the legitimate acquisition and use of software.

Commentary and examples

4.1. The fight against the underground economy of counterfeit and pirate goods requires diligence and co-operation among all stakeholders—governments, IP owners, other public authorities and companies in every part of the supply chain. Co-operation with rights owners/software vendors as well as other relevant private-sector and government stakeholders can produce

tremendous synergies for a government as it develops and maintains effective IP-management policies, including for software.

4.2. As the ICC/BASCAP Guidelines point out, it may also be necessary for government departments to co-operate with IP rights owners or law enforcement officials if counterfeits are found or other problems of infringement arise. Such co-operation may include, for example, producing IP licences and other information relating to suspect articles, orders or activity.

4.3. Numerous industry bodies, including the ICC/BASCAP and industry-specific associations, private sector vendors, accountancy firms and other consultancies can provide general or specific model programmes at no cost or for a nominal charge, or paid individual advice, to help governments design and implement their IP management policies, procedures and practices.

5. References: Excerpts from G8 Reports and Declarations

G8 Intellectual Property Experts Group Report of Discussions
L'Aquila, Italy, July 2009
http://www.g8italia2009.it/static/G8_Allegato/ITALY%20G8%20IPEG%20Final%20Report,0.pdf

Okinawa Charter commitment on Use of Software in full compliance with Intellectual Property Rights

Governments have a special duty to set an example in the fight against counterfeiting and piracy. In line with this view, at the Hokkaido Toyako Summit in 2008 leaders agreed to reaffirm the Okinawa Charter commitment to ensure that governments use software in full compliance with Intellectual Property rights protection.

The IPEG (Intellectual Property Experts Group) has elaborated and approved the attached set of guidelines (ATT.1) to contribute to reducing the risk of public networks being used to infringe IP rights.

G8 Guidelines for Governments Use of Software in Compliance with Intellectual Property Rights

Responding to advances in Information and Communications Technology, the G8 leaders at the 2000 Kyushu-Okinawa Summit adopted the Okinawa Charter on Global Information Society, which calls for governments to use software in full compliance with Intellectual Property rights protection. At the 2008 Hokkaido-Toyako Summit, the G8 leaders renewed this commitment, and called upon other countries to follow it.

Since Okinawa, technological developments – including the advent of peer-to-peer file sharing – have posed new challenges and concerns.

Governmental networks constitute a significant portion of Information Technology (IT) and Internet resources, and are thus exposed to the risks and problems associated with Intellectual Property infringement.

By reaffirming the commitments made in the Okinawa Charter, and ensuring that laws, regulations, and policies are in place to reduce the risk that public computing resources are used to infringe IP rights, governments can set an example for the private sector and for IT users in the fight against counterfeiting and piracy, and, at the same time, safeguard the interests of security and transparency of their own administrations.

In line with this view, the Intellectual Property Expert Group developed the following set of guidelines as an instrument to improve the protection of IP rights within public administrations.

Guidelines:

- **Software Products**
  Governments shall not violate Intellectual Property rights in the acquisition and deployment of software, and will establish the necessary measures to ensure the fulfilment of this commitment. The competent authorities should take measures to verify that computers employed by public administrations be exclusively provided with legitimate software.

- **Use of Government Computer Networks**
  The competent authorities should establish the necessary measures to ensure that the use of government computer networks, including, for example, those operated by contractors, does not violate Intellectual Property rights.

- **Information and Awareness**
  Public administrations should undertake campaigns and/or informational initiatives to raise employees' awareness about the importance of Intellectual Property rights for innovation and the development of new products, with a view to encouraging the appropriate use of Information Technology.

  Public employees should be informed about network operating rules and procedures and the consequences of the illegal or improper use of public computer systems.

- **Public-Private Sector Collaboration**
  Aware of the crucial importance of public procurement in fostering innovation in the software industry, governments may collaborate with the private sector and other stakeholders to share best practices related to the legitimate acquisition and use of software.

G8 Leaders Declaration: Responsible Leadership for a Sustainable Future
L'Aquila, Italy, 8 July 2009
http://www.g8italia2009.it/static/G8_Allegato/G8_Declaration_08_07_09_final,0.pdf

Innovation and knowledge are key factors for supporting the recovery and putting the world economy on a more sustainable growth path…. [A]n enabling policy and business environment where intellectual property rights (IPR) are respected is necessary to promote innovation, knowledge, entrepreneurship and creativity…. Counterfeiting and piracy continue to pose a threat to the global economy, public health and welfare. For this reason, we

welcome the results of work carried out by our experts, as reflected in the G8 Intellectual Property Expert Group Report of Discussion.

G8 Hokkaido Toyako Summit Leaders Declaration
Hokkaido Toyako, Japan, 8 July 2008
http://www.mofa.go.jp/policy/economy/summit/2008/doc/doc080714__en.html

Effective promotion and protection of IPR are critical to the development of creative products, technologies and economies. We will advance existing anti-counterfeiting and piracy initiatives…. We reaffirm our commitment on government use of software in full compliance with the relevant international agreements and call on other countries to follow our commitment.

G8 Okinawa Charter on Global Information Society
Kyushu-Okinawa Summit, Japan, July 2000
http://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf

In order to maximize the social and economic benefits of the Information Society, we agree on the following key principles and approaches and commend them to others:

- Protection of intellectual property rights for IT-related technology is vital to promoting IT-related innovations, competition and diffusion of new technology; we welcome the joint work already underway among intellectual property authorities and further encourage our experts to discuss future direction in this area;
- Governments' renewed commitment to using software in full compliance with intellectual property rights protection is also important.

Annex 2:
Avoiding Counterfeits in Government Procurement

Overview

Governments, like businesses and consumers, can be the victim of counterfeiting and piracy. Counterfeit and pirated products and services sometimes get delivered as part of government procurement bids for items such as electronics, defence equipment, spare parts, software and medicines. The incentives for suppliers to make more money by delivering cheap counterfeits, and the temptation of government buyers to buy cheap components at times regardless of origin or quality, are obvious. All kinds of risk and damage can ensue, however, including failed equipment and systems, security problems, lost time, wasted public funds and in many cases threats to human health and life.

> *"Almost anything is at risk of being counterfeited."*
>
> **US General Accountability Office,** http://www.gao.gov/products/GAO-10-389
>
> *"The bottom line is that [the counterfeiters'] motivation was simply about the money and ultimate greed."*
>
> **Marcy Foreman, Director of Office of Investigations, US Immigration and Customs Enforcement,** http://news.bbc.co.uk/1/hi/health/7865569.stm.

Governments can and should implement effective policies to discourage, detect and redress counterfeit and pirated products and services in public procurement. Business Action to Stop Counterfeiting and Piracy (BASCAP), an initiative of the International Chamber of Commerce (ICC), has developed a broad set of Intellectual Property (IP) Guidelines to provide information on practical steps that businesses and other organisations can take to manage copyrighted, trademarked and other IP-protected goods and services effectively within their organisations. See http://www.iccwbo.org/bascap/index.html?id=24276.

This Annex to the ICC/BASCAP IP Guidelines describes particular issues and strategies involved in addressing counterfeiting and piracy in public procurement. Based on the general principles and practical suggestions described in the IP Guidelines, this Annex describes particular ways in which governments can protect against and address counterfeiting and piracy in their procurement system, contracts and compliance mechanisms.

The significance and scale of counterfeiting and piracy in the public-procurement supply chain has recently come into sharp focus. Two US government departments reviewed the problem of counterfeits in defence procurement in 2010, finding that "Almost anything is at risk of being counterfeited,"[1] and lamenting that "DOD [the Department of Defense] does not currently have a policy or specific processes for detecting and preventing counterfeit parts. Existing procurement and quality-control practices used to identify d eficient parts are limited in their ability to prevent and detect counterfeit parts in DOD's supply chain."

A European Commission survey found 27 separate cases of counterfeit medicines entering the legitimate supply chain between 2001 and 2005 in the EU, where pharmaceuticals are often procured directly by government departments or government-run medical facilities. While the World Health Organisation and the United Nations have estimated that 1% of the medicines in circulation in such developed countries are fake, the incidence of counterfeits rises to 50% of the drugs sold in many developing countries and over the internet.[2]

Governments sometimes use the term 'counterfeit' broadly to include not just intellectual-property related misrepresentations—falsely branded items, and other items manufactured or supplied in violation of trademark, copyright or other IP rights—but also to include any misrepresentation of an item's quality and performance.[3] This paper focuses on public procurement of IP-related counterfeited and pirated goods, but these items also routinely involve misrepresentations as to quality and performance. The strategies outlined in this paper for addressing IP-based counterfeits are also useful, therefore, in addressing counterfeiting even if it is defined more broadly with respect to public procurement.

The many kinds of counterfeited and pirated products found to have been acquired by government procurement, and the kinds of risks that these pose, can be seen in the following examples.

- **Electronics products and components.** Counterfeit Cisco **network routers and components** have been found to have been procured by several US government agencies, including the Air Force, Marine Corps, US Navy, Federal Aviation Authority, their defence contractors and even the FBI. An investigation led by the FBI and involving five other government agencies in the US and Canada led to the issuance of 36 search warrants, and the discovery of 3,500 counterfeit Cisco network components with an estimated retail value of more than $3.5 million over the two-year period 2006-2008. More than fifteen criminal cases were brought, with a total of 10 criminal convictions. This was part of a broader FBI initiative that had involved more than 400 seizures of counterfeit Cisco network hardware and labels with an estimated retail value of more than $76 million.[4]

  Other counterfeit electronics supplies that have turned up in government procurement have included **microprocessors** for an F-15 fighter jet control computer, **Global Positioning System oscillators** for military systems, electronic **amplifiers, diodes** and **micro-circuits.**[5] About two-thirds of the instances of suspect and confirmed counterfeit parts reported by the US Department of Defense involved electronics parts or fasteners.[6]

Figure 1. Counterfeit Network Interface Cards

(FBI, FBI Criminal Investigation: Cisco Routers, http://www.abovetopsecret.com/forum/thread350381/pg1, attributed to Andover Network Liquidators, *http://www.andovercg.com/services/cisco-counterfeit-wic-1dsu-t1.shtml.*

These types of electronics counterfeits in the supply chain represent several different types of risks for the governments that procure them. Besides the normal problem that such components may not be durable or may not work at all, counterfeit electronics can give a less-than-optimal performance, produce incorrect results, or even introduce a severe safety risk for those who depend on them. For example, counterfeit GPS systems installed in military control systems "could cause mission failure,"[7] noted the US General Accountability Office (GAO), with obvious risks to life and limb.

Even more worrying, counterfeit electronics have the potential of introducing security and intelligence risks into government computer systems. An FBI investigation has identified these risks as including the potential to allow remote users to gain access to otherwise secure government systems, to weaken governments' encryption systems, and to cause systems to fail.[8]

- **Software supply and use.** Governments sometimes find that they have been supplied counterfeit or pirated (i.e. unlicensed) software products, or have been supplied services by vendors whose systems use such software. A local government in Scotland that allegedly had been supplied counterfeit Microsoft Office product licences by an IT vendor found itself subject to a civil settlement of £42,500 and required to purchase an additional 470 software licences at a cost of £102,229 in 2002.[9] That same year, ten British police constabularies and even Scotland Yard's "Special Branch" were supplied copies of allegedly counterfeit software with a £1.3 million computer system.[10]

  Risks to governments that purchase or rely on vendors that use counterfeit or pirated software include:

  - quality, reliability and performance risks (counterfeit software has a high incidence of viruses, Trojan horses and other malware),
  - legal challenges and penalties, and
  - inadequate control over IT systems, resources and costs.[11]

- **Defence and security products and spare parts.** Spare parts are among the most commonly counterfeited items supplied under government procurement bids related to defence and security. The US government's recent review of various problems with Defense Department procurement of parts and components found that counterfeits had been supplied in bids for such items as **self-locking nuts,** titanium **aircraft parts**, aluminium **vehicle and weapons parts,** hermetically sealed **microwave boxes, air conditioning components,** and even **seatbelts.** Other counterfeit automobile parts including **brake shoes** made from seaweed, as well as counterfeit **body armour** represented as Kevlar® brand fibre material that was nothing of the sort, have also been supplied in government tenders.[12]

  As the GAO pointed out, such supplies, components and parts have the potential to cause a serious disruption to supply chains, delay on-going missions, affect the integrity of weapon systems, pose risks to civilian as well as military programmes, result in property loss, and cause human casualties.

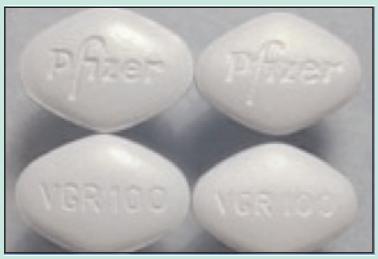
- **Medicines and medical devices.** Even in countries where pharmaceuticals and medical supplies are highly regulated and their procurement and sale are carried out or funded by the

government, counterfeits can and do creep into the supply chain. "All kinds of medicines have been counterfeited – branded and generic – ranging from medicines for the treatment of life-threatening conditions to inexpensive generic versions of painkillers and antihistamines," reports the World Health Organisation.[13]

Among the estimated 1% of counterfeit products that have found their way into Europe's extensively state-funded medical procurement systems have been counterfeit medicines for **heart conditions** and **strokes** (Plavix (clopidogrel)), **prostate cancer** (Casodex (bicalutamide)), **high cholesterol** (Lipitor), **obesity** (Reductil (sibutramine)), **asthma** (Seretid), and **schizophrenia** (Zyprexa (olanzapine)), not to mention sexual dysfunction medicines sold both within and outside traditional medical supply chains. Among medical devices, fake **intra-ocular lenses, contact lenses, continence** products, **glucose test strips, dental filling material, ice packs, insulin needles,** and even **HIV test kits** have been discovered in Europe.[14]

Figure 2. Counterfeit Medicines.
This counterfeit Viagra® medicine was found in Hungary. Instead of the appropriate active ingredient, these counterfeits contained only amphetamine—commonly known as "speed".

Pfizer, Case Study: Counterfeit Contents, http://media.pfizer.com/files/products/CounterfeitContents.pdf.



Here the risks to human health and life are painfully obvious. The contents of counterfeits can be dangerous or can lack active ingredients. Their use can result in treatment failure, or can build up resistance to legitimate medicines where the active ingredient in the counterfeit is too low. They can even cause death. Counterfeit versions of the narcotic drugs fentanyl and oxycodone have resulted in numerous deaths in the US and Europe.[15]

Unlike genuine medicines where any problems with the manufacturing process can be traced and dealt with by a known manufacturer, counterfeit medicines are made by people with the intent to mislead. Marcy Foreman, who deals with such counterfeits as Director of the Office of Investigations for US Immigration and Customs Enforcement, put the problem succinctly to the BBC: The bottom line is that counterfeiters' motivation is "simply about the money and ultimate greed".[16]

The kinds of procurement and asset-management policies described in ICC/BASCAP's IP Guidelines as beneficial for companies that deal with IP-based goods and services are also relevant to governments as they seek to discourage, detect and redress counterfeit and pirated products and services in public procurement.

In line with the five major types of strategies and procedures recommended in the IP Guidelines—dealing with policy, awareness, supply chain, security and compliance—the steps that governments should consider with respect to their own procurement policies and practices are described below. Some illustrative examples are provided with respect to practices already in place in some countries. Also included are references to recent government recommendations that have emerged from the growing world-wide concern that counterfeits increasingly are leaking into governments' supply chains.

1. Government policy

The law should be clear that the supply and use of counterfeits pursuant to government procurement is illegal. A clear government policy, co-ordinated well among relevant departments, is vital.

Guidance

1.1 Illegality of counterfeits. In some countries, it appears that the supply of counterfeit products or components pursuant to government tender is not specifically illegal. Germany, Spain and Lithuania have specific legislation barring 'counterfeit medicines', for example, but most other EU countries rely on a patchwork of intellectual property and medicines marketing authorisation laws to address counterfeits.[17] It is important that procurement law specifically and clearly prohibits the supply of counterfeits of all kinds of products and components.

1.2 Form of prohibition. The form of the rule barring tender of counterfeits can be a simple prohibition of the tender of any goods, components or other material as to which the supply or use would violate the intellectual property rights of a third party. Alternatively, such a requirement may be mentioned specifically as part of broader conformance or anti-fraud rules that prohibit the tender of items as to which the identity, history, source or quality have been falsified. It is also important that sanctions be included that are sufficient and sufficiently robust to deter non-compliance. China's draft Implementation Rules for Government Procurement Law provide, for example, that a supplier that tenders fake products is subject to disgorgement of profits, a fine, exclusion from procurement bids for one to three years, cancellation of its business licence, and criminal prosecution.[18]

1.3 Lawful use. Governments' policies among their own departments and employees also should be clear that the acquisition and/or use of materials that are counterfeit or that otherwise infringe intellectual property rights is not tolerated. A further description of these types of policies can be found in the ICC/BASCAP IP Guidelines and its Annex 1: G8 Guidelines for Governments Use of Software in Compliance with Intellectual Property Rights. Another recommended policy along these lines, which has emerged in recent discussions among US government departments, is to require that vendors also comply with intellectual property laws with respect to the services they supply to the government, for example by using only legal copies of software in their business.[19]

1.4 **Responsibility and co-ordination.** Government procurement by definition spans a range of departments and responsibilities. A co-ordinated effort among all relevant departments, with clear lines of responsibility for developing needed policies and procedures, is important for ensuring a consistent approach and maximum effectiveness in discouraging, detecting and redressing counterfeits in public procurement. The US Government, for example, has recently convened a working group on this issue consisting of seven government departments and led by the Administrators of the Government Services Administration and Federal Procurement Policy, the White House Intellectual Property Enforcement Co-ordinator, and the Undersecretary of Defense.

A specific unit within the UK Government's Medicines and Healthcare Products RegulatoryAgency (MHRA) has been assigned responsibility for investigating, identifying and co-ordinating enforcement against counterfeit medicines and medical devices in the legitimate and illegitimate supply chains, working with the Department of Works and Pensions, Trading Standards Officers, and other government departments pursuant to a comprehensive Anti-Counterfeiting Strategy.[20]

2. Education and awareness

Government employees, vendors and even the public can benefit from information and training on the rules and risks of counterfeits in public procurement.

Guidance

2.1 **Internal awareness.** Understanding the rules and risks and being able to identify counterfeits is an important component of reducing their incidence in government procurement. The US GAO's enquiry received reports from several Defense Department officials that "staff responsible for assembling and repairing equipment are not trained to identify counterfeit parts." This has begun to be addressed, for example, by a department-wide team that is not only reviewing processes and procedures for the handling and storage, detection, disposal and reporting of counterfeit parts, but also developing training materials and courses to increase internal awareness of counterfeit parts and of detection techniques.[21]

2.2 **Supplier notification/awareness.** The ICC/BASCAP IP Guidelines recommend that companies notify suppliers that the company complies with IP laws and expects them to do the same. Similar notifications are useful for governments to make to their suppliers.

2.3 **Consumer awareness.** With respect to certain types of goods subject to government procurement, particularly medicines and medical devices, governments have found it useful to provide training and other information to vendors and even consumers about counterfeits. For example, the UK MHRA provides information not only to pharmacists on the risks, recognition and reporting of counterfeits, but also puts information on its website about specific counterfeit medicines found in the UK supply chain as a warning to the general public.[22]

3. Supply chain management

Procurement contracts should specifically provide for prohibitions, warranties and sanctions related to the supply and/or use of counterfeits. Due diligence on vendors in the supply chain can help to weed out counterfeit supply.

Guidance

3.1 Contractual provisions. As described in the ICC/BASCAP IP Guidelines with respect to supply contracts in the private sector, it is important that government procurement tenders and contracts themselves include specific clauses that deal with the risks of counterfeits. These can include such clauses as prohibitions on the supply and/or use of counterfeits, warranties that such requirements have been complied with, and meaningful contractual sanctions that cover the breach of these provisions. Again, these can be dealt with as IP-specific clauses, or detailed as part of broader conformance and anti-fraud clauses.

3.2 Required licences. Where relevant, the certifications of compliance or similar documentation supplied by government contractors can also usefully include copies or other written proof of requisite IP licences or other rights, as described in the ICC/BASCAP IP Guidelines.

3.3 Due diligence. While tools such as marketing authorisations to identify reliable vendors are common in the field of medicines, the benefits of using approved suppliers are often not used to good advantage in many areas of public procurement. The aerospace and electronics parts industries have been developing helpful recommended policies in this area, for example, standards that encourage the procurement of components from approved supplier lists (e.g. the original manufacturer, approved distributors, and others that have agreed to abide by policies and procedures laid down in the standard designed to mitigate counterfeits), and/or to exercise due diligence with respect to non-vetted vendors. The US Department of Defense has adopted SAS Standard AS5553 along these lines.[23]

4. Asset management and security

Supply traceability among governments and suppliers, and adequate asset management and physical and IT security, can reduce the risks and consequences of counterfeits.

Guidance

4.1 Traceability. Surprisingly, the origin of products and components that governments procure is often not readily traceable. Policies such as SAS Standard AS5553 described above encourage good vendor and parts management and recordkeeping in the supply chain, such that any products or parts discovered can be reliably traced to their source. This helps both to prevent and to redress the problem of counterfeits.[24]

4.2 Asset management, security. More generally, good internal management and recordkeeping with respect to intellectual-property based products, components and services, as well as effective physical and IT security to prevent violations and unauthorised access, are vital in the government's as well as the private sector's efforts to reduce the incidence and consequences of counterfeiting. ICC/BASCAP's IP Guidelines describe several types of helpful policies and procedures in these areas.

5. Compliance and audit

Regular audits of goods tendered, investigation and enforcement against counterfeits, and co-operation with public enforcement bodies and the private sector, are also important practices to deal with counterfeits in public procurement.

Guidance

5.1 Quality conformance and audits. Government procurement programmes regularly include quality conformance procedures and checks on goods and components supplied, as well as more in-depth audits of vendor performance. These should include checks for counterfeit parts and components, and practices that inadequately discourage the supply of such items. The United Nation's International Narcotics Control Board recommends, for example, "regular inspection of entities involved in the manufacture, trade and distribution of pharmaceuticals". Similar checks on vendors of other types of goods and components may be appropriate where there is reason to believe counterfeits have been or may be supplied.

5.2 Investigation, enforcement. Good laws and procedures rarely can be fully effective without prompt investigation and deterrent enforcement against violations. Some governments have set up specialised units within their procurement-related departments specifically to investigate and redress violations such as the supply of counterfeits, for example, the MHRA in the United Kingdom mentioned above.

5.3 Co-operation with private sector. As the developers of most of the items purchased by governments, the private sector has a wealth of information about how to recognise counterfeit products and components, the sources and distribution patterns of such items, training courses and materials, and information about policies and best practices that can be adopted to discourage, detect and redress counterfeits. The US Government's GAO report lists several private-sector organisations that can provide helpful public-private co-operation related to counterfeits in government procurement, including not only ICC/BASCAP but also the Aerospace Industries Association, Electronic Industry Citizenship Coalition, International Anti-Counterfeiting Coalition, SAE International, Semiconductor Industry Association, and others.[25]

5.4 Monitoring/updating policies. Discouraging, detecting and redressing the supply and use of counterfeits and other infringing items in government procurement is, unfortunately, a challenge that cannot be fixed once for all time. As the ICC/BASCAP IP Guidelines explain with respect to IP-related policies more generally, it is important for governments to engage in on-going monitoring of their anti-counterfeiting policies related to procurement, to correct problems, and to refine their policies from time to time as needed, in order to make sure that they indeed work and that they are in fact followed by government personnel and vendors alike.

References

[1] US Government Accountability Office, Report to Congressional Requesters, Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts, p. 2 (March 2010) ("GAO 2010"), http://www.gao.gov/products/GAO-10-389 ; see also U.S. Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics (Jan. 2010), http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

[2] See, e.g., WHO, International Medical Products Anti-Counterfeiting Taskforce, http://www.who.int/mediacentre/factsheets/fs275/en/index.html.

[3] SAE Aerospace Standard 5553, for example, defines a counterfeit part as a suspect part that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by a supplier in the supply chain. By contrast, one US Defense Logistics Agency supply centre defines a part as counterfeit only when it misrepresented the part's trademark. (GAO 2010, p. 2).

[4] J. Markoff, F.B.I. Says the Military Had Bogus Computer Gear, New York Times (9 May 2008), http://www.nytimes.com/2008/05/09/technology/09cisco.html?_r=1&ref=technology, citing ATSNews, FBI Fears Chinese Hackers Have Back Door Into US Government & Military, http://www.abovetopsecret.com/forum/thread350381/pg1; US Dep't of Justice, Departments of Justice and Homeland Security Announce International Initiative Against Traffickers in Counterfeit Network Hardware (9 Feb. 2008), http://www.justice.gov/opa/pr/2008/February/08_crm_150.html.

[5] GAO 2010, pp. 7-8.

[6] GAO 2010, p. 7.

[7] GAO 2010, p. 24.

[8] Markoff 2008, ATS News 2008.

[9] Cliff Saran, How a council got clobbered for software piracy, Computer Weekly (21 Jan. 2002), http://www.computerweekly.com/Articles/2002/01/21/184723/How-a-council-got-clobbered-for-software-piracy.htm.

[10] Richard Alleyne, 'Pirated' software at Special Branch, Daily Telegraph (20 Nov. 2002), http://www.telegraph.co.uk/news/uknews/1413725/Pirated-software-at-Special-Branch.html; see also BBC, How Cyber Piracy Affects You (9 Apr. 2003), http://news.bbc.co.uk/1/hi/uk/2924531.stm.

[11] BSA, Government Guide For Software Management, http://www.bsa.org/~/media/C72B329D6F7E4B46A7467DE0151210A1.ashx

[12] GAO 2010, pp. 25-26.

[13] WHO, Counterfeit Medicines, http://www.who.int/mediacentre/factsheets/fs275/en/index.html.

[14] A.C.P. de Bruijn, C.G.J.C.A. de Vries, H.P.H. Hermsen, Counterfeit medical devices: A risk indication, RIVM National Institute for Public Health and the Environment, Letter report 360060001/2009 (August 2009), http://www.rivm.nl/bibliotheek/rapporten/360060001.pdf.

[15] Statement by Dr. P. Emafo, President of the International Narcotics Control Board, Third Global Congress on Combating Counterfeiting and Piracy (30-31 January 2007), http://www.wipo.int/enforcement/en/global_congress/docs/philippe_emafo.doc.

[16] BBC, How Fake Drugs Got into the NHS, (3 Feb. 2009), http://news.bbc.co.uk/1/hi/health/7865569.stm.

[17] Europe Economics, Compilation of Material Relating to Counterfeit Medicines (8 Jul. 2008), http://ec.europa.eu/health/files/counterf_par_trade/conterfeit_doc/11-11-2008/counterfeit-study-main-report_en.pdf.

[18] See http://lawprofessors.typepad.com/.../government-procurement-regulations---draft-for-comment---1-11-10-en.pdf.

[19] See Executive Office of the President, 2010 Joint Strategic Plan on Intellectual Property Enforcement, pp. 7-8 (June 2010) ("Use of Legal Software by Federal Contractors"), http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf.

[20] Medicines And Healthcare Products Regulatory Agency (MHRA), Anti-Counterfeiting Strategy 2007-2010, http://www.mhra.gov.uk/home/groups/ei/documents/websiteresources/con2033156.pdf.

[21] GAO 2010, pp. 9-10.

[22] MHRA, Guidance for Pharmacists: Counterfeit Medicines, http://www.mhra.gov.uk/home/idcplg?IdcService=GET_FILE&dDocName=CON2023831&RevisionSelectionMethod=LatestReleased; MHRA, Counterfeit Medicines and Devices, http://www.mhra.gov.uk/Safetyinformation/Generalsafetyinformationandadvice/Adviceandinformationforconsumers/Counterfeitmedicinesanddevices/index.htm.

[23] See SAE, Standard AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, http://standards.sae.org/as5553; TechAmerica, Engineering Bulletin TB-0003, http://www.techstreet.com/standards/TechAmerica/TechAmerica_TB_0003?product_id=1608325; SAS, DOD adopts SAE's AS5553 standard on counterfeit electronic parts (14 Oct. 2009), http://www.sae.org/mags/aem/7058.

[24] See Phil Zulueta, Counterfeit Electronic Parts, Avoidance, Detection, Mitigation and Disposition: AS5553 Standards Development Progress (Oct. 2008), http://supplychain.gsfc.nasa.gov/2008/SC2008-Zulueta_a.ppt.

[25] GAO 2010, pp. 15-18.

Please visit the BASCAP website for an electronic copy of the IP Guidelines for Business in various languages, and updated information, at www.iccwbo.org/bascap.

Business Action to Stop Counterfeiting and Piracy is a business initiative, created, led and funded by the world business community, specifically brand owners, and organized by the International Chamber of Commerce, to raise public and political awareness about counterfeiting and piracy, encourage government action and promote respect for intellectual property.

To learn more about membership in ICC / BASCAP, please contact
Jeffrey P. Hardy
Coordinator, BASCAP
E-mail: bascap@iccwbo.org

Published in March 2011 by International Chamber of Commerce.

International Chamber of Commerce
38, cours Albert 1e, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 29 42
E-mail icc@iccwbo.org Website www.iccwbo.org

ICC Publication No. 848
ISBN: 978-92-842-0060-3

The International Chamber of Commerce

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The fundamental mission of ICC is to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the last century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rules-setting, dispute resolution and policy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on vital technical and sectoral subjects. These include financial services, information technologies, telecommunications, marketing ethics, the environment, transportation, competition law and intellectual property, among others.

ICC enjoys a close working relationship with the United Nations and other intergovernmental organizations, including the World Trade Organization, the G20 and the G8.

ICC was founded in 1919. Today it groups hundreds of thousands of member companies and associations from over 120 countries. National committees work with their members to address the concerns of business in their countries and convey to their governments the business views formulated by ICC.

For information on how to join ICC, visit the ICC website (iccwbo.org) or contact the ICC Membership Department in Paris.

38 cours Albert 1er, 75008 Paris, France
Tel: +33 (0)1 49 53 28 28 Fax: +33 (0)1 49 53 28 59
E-mail icc@iccwbo.org Website www.iccwbo.org