INTERPOL Intellectual Property Rights Program

Consultation Document

INTERPOL Database on International Intellectual Property (DIIP) Crime

INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector

Lyon, June 6, 2008

INTERPOL Intellectual Property Rights Program

INTERPOL Database on International Intellectual Property (DIIP) Crime

The INTERPOL Database on International Intellectual Property (DIIP) Crime is an autonomous iBase database containing information about transnational and organized intellectual property (IP) crimes.

It has been specifically developed to be a depository for private sector industry information about transnational and organized IP crime. The Database on International Intellectual Property (DIIP) Crime neither competes with established public sector IP crime databases nor duplicates existing IP crime data collection mechanisms.

Data contained in the database will be subjected to criminal analysis to identify links between transnational and organized cross-industry sector IP criminal activity; facilitate criminal investigations; and, develop regional and global strategic IP crime reports.

INTERPOL does not disclose information contained in Database on International Intellectual Property (DIIP) Crime. Participating industries receive feedback in the form of referrals indicating that two or more industries are being targeted by the same transnational organized criminals.

Disclosure then takes place at the discretion of, and by, the industry owning the information in accordance with local data protection requirements.

INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector

The INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector complements the Database on International Intellectual Property (DIIP) Crime.

The purpose of the INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector is to provide IP crime affected private sector entities with guidance about the type of information they should consider collecting about transnational and organized IP crime attacks on their interests.

In the event that private sector entities adopt the Minimum Global Standard it will enable the information to be easily assimilated into the INTERPOL Database on International Intellectual Property (DIIP) Crime in accordance with DIIP Data Handling and Referral Procedures.

The Minimum Global Standard will also enable private sector entities to share information about transnational and organized IP crime with each other more effectively.

Appendices
The attached appendices provide detailed information about the INTERPOL Database on International Intellectual Property (DIIP) Crime and INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector

1. Database on International Intellectual Property (DIIP) Crime and INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector - Frequently Asked Questions (Appendix 1)

2. Database on International Intellectual Property (DIIP) Crime - Data Handling and Referral Procedures (Appendix 2)

3. Database on International Intellectual Property (DIIP) Crime - Recommended Agreement Letter Template (Appendix 3)

4. INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector (Appendix 4**)**

Intellectual Property Rights Project
I.C.P.O. – INTERPOL
General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France

Tel : +33 4 72 44 57 95
Fax : +33 4 72 44 57 97

www.interpol.int

INTERPOL Intellectual Property Rights Program

Appendices

1. **Database on International Intellectual Property (DIIP) Crime and INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector - Frequently Asked Questions (Appendix 1)**

2. **Database on International Intellectual Property (DIIP) Crime - Data Handling and Referral Procedures (Appendix 2)**

3. **Database on International Intellectual Property (DIIP) Crime - Recommended Agreement Letter Template (Appendix 3)**

4. **INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector (Appendix 4)**

Lyon, June 6, 2008

Appendix 1.

INTERPOL Database on International Intellectual Property[1] (DIIP) Crime - Data Handling and Referral Procedures

And

INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector

Frequently Asked Questions (FAQ)

Q. Why is INTERPOL so interested in collecting data about counterfeiting and piracy from IP crime affected private sector industries?

A. Transnational organized criminals are manufacturing and distributing counterfeit and pirate goods on an industrialized scale. Despite this there is an absence of reliable data to inform policy makers in governments and law enforcement about the true nature and extent of the problem. This prevents law enforcement and affected industries focusing scarce collective resources where they will be most effective. DIIP will fill the current cross-industry sector information void identified by the OECD.[2]

Q. Why introduce DIIP when the customs authorities already collect information about seizures of counterfeit and pirate products?

A. The World Customs Organization (WCO) collects data about customs seizures by customs administrations in its member countries. EC TAXUD[3] collects information about customs seizures within the European Union. These sources are important, but are limited as they solely relate to customs seizures. Customs seizures do not provide a comprehensive overview of the activities of transnational organized criminals who systematically manipulate counterfeit and pirate goods to generate significant profits.

Q. Is DIIP in competition with other public or private sector databases?

A. No, there is no other database that provides this service for stakeholders and INTERPOL is uniquely able to provide it

[1] Intellectual property (IP) crime is a generic term used by INTERPOL to describe all types of counterfeiting and piracy

[2] The Economic Impact of Counterfeiting and Piracy, Organization for Economic Co-operation and Development, 2007

[3] European Commission Taxation and Customs Union

Q. How will it help collective efforts to combat transnational and organized IP crime?

A. INTERPOL works as a catalyst to encourage police, customs, international organizations, the public health sector, cross-industry representative bodies, IP crime affected industries and other stakeholders to work together to combat transnational organized counterfeiting and piracy. It does this by facilitating and coordinating regional law enforcement interventions[4] in the activities of transnational organized criminals in partnership with INTERPOL member countries and affected industries or the public health sector[5].

These operations have been successful and delivered benefits for all stakeholders. To maximize benefits arising from these successes for all stakeholders there is a need to use DIIP to systematically act as a catalyst for these interventions on the basis of reliable information for action.

Q. What are the benefits for participating private sector industries?

A. Typically IP crime affected industries will work together with other industries in their industrial sector to combat transnational organized criminals who attack their commercial interests. This includes exchanging information when it is appropriate to do and in accordance with relevant data protection requirements. However, it is unusual for one industry sector to do this with another industry sector.

Transnational organized criminals are not restrained by these arrangements or national borders and manipulate all counterfeit or pirate products to generate profits. As a result IP crime affected industries are often unknowingly attacked by the same transnational organized criminals. DIIP will identify these situations and use a system of referrals to enable affected industries to pool investigative resources and focus them where they will be most effective.

Q. Does INTERPOL charge participating industries a fee for processing and storing their information?

A. No.

[4] Operation Jupiter – South America II deployed in Argentina, Brasil, Chile, Paraguay and Uruguay resulted in the seizure of contraband, counterfeit and pirated goods valued at over US$35 Million and disrupted associated transnational organized criminality.

[5] "An Epidemiological Collaborative Investigation into the Criminal Fake Artesunate Trade in South East Asia", Pubic Library of Science, February 2008/Volume 5/ Issue 2 (http://medicine.plosjournals.org/perlserv/?request=get-document&doi=10.1371/journal.pmed.0050032)

Q. A common complaint from financial institutions is that there is no feedback about information submitted to the authorities to meet money laundering related obligations. Will participating private sector industries receive feedback on information submitted to DIIP?

A. Yes. Participating industries will receive feedback in the form of referrals indicating that two or more industries are being targeted by the same transnational organized criminals. (See: Data Handling and Referral Procedures – Section 6: Disclosure of Information and Referrals)

Q. What performance measures does INTERPOL use to measure the effectiveness of DIIP?

A. There are currently five performance measures to measure DIIP effectiveness from the number of submissions received from participating industries through to the number of referrals made to them by the INTERPOL IP Crime Unit. (See: Data Handling and Referral Procedures – Section 8: Performance Measurement)

Q. What regulatory framework does INTERPOL use to regulate data handling and the exchange of information?

A. As an international organization INTERPOL has to comply with its Rules on the Processing of Information for the Purposes of International Police Co-operation and the texts to which they refer. DIIP meets the aims of the International Criminal Police Organization - INTERPOL which are to ensure and promote the widest possible mutual assistance between all criminal police authorities. (Article 2 of the Organization's Constitution).

Article 6.2.c. of the Rules on the Processing of Information for the Purposes of International Police Co-operation provide that specialized databases may only be set up when it is necessary and relevant for reasons of a technical, legal or security nature, or to facilitate the processing of information, or for the information to be studied in the context of a project concerning information or a crime analysis operation.

Q. Industries affected by counterfeiting and piracy have duties under national data protection legislation to process information in an appropriate manner. Does this prevent affected industries from submitting information to INTERPOL?

A. No. In most jurisdictions it is permissible to share information with police for the purposes of preventing or detecting crime within the limits of national legislation of the source.

Q. What type of information does INTERPOL want from IP crime affected industries?

A. The express purpose of DIIP is to collect reliable information about transnational organized criminals from IP crime affected industries. Industries often know the identity of the persons or groups who attack them as these are one and the same people that affected industries take civil actions against to protect their intellectual property and enforce rights.

Information collected to support civil actions is expensive and typically once the civil action is complete the information is not used for any other purpose. This information is a valuable resource since it contains information about transnational organized criminals. Pooling the information in DIIP adds value to the information and improves its cost effectiveness. Pooled information is searched to identify links between all IP crime affected industries and can then be used for the collective benefit of all stakeholders.

Q. Will participating industries be able to look at the information contained in DIIP?

A. No. The priority is to ensure that confidential and proprietary information provided by participating industries is not disclosed. Consequently representatives of participating industries cannot view the contents of DIIP.

The exception to this rule is during the quality assurance process after receipt of information from a particular industry when it may be necessary for consultation to take place to provide clarification and ensure the accuracy of the information. The consultation will only relate to that industry's information which will not be entered into DIIP until the quality assurance process has been completed.

Q. How does INTERPOL protect the confidentiality and proprietary interests of information submitted to DIIP by participating private sector industries? Who has access to DIIP?

A. DIIP is an autonomous database and responsibility for it rests with the INTERPOL IP Crime Unit. Access to DIIP is restricted to members of the IP Crime Unit and nominated IT technicians responsible for database maintenance (See: Data Handling and Referral Procedures – Section 2: Control and Maintenance of DIIP)

Q. INTERPOL processes police information received from member countries using the INTERPOL Criminal Information System (ICIS). Will information received from participating industries be stored in ICIS?

A. DIIP is an autonomous database and participating industry information is processed separately from the police information stored in ICIS. At no time is participating industry information stored in ICIS. (See: Data Handling and Referral Procedures – Section 4: Comparison between DIIP and ICIS)

Q. Does INTERPOL disclose information contained in DIIP?

A. INTERPOL does not disclose information contained in DIIP. In the event links between participating private sector organizations and other forms of ongoing criminality are identified the IP Crime Unit will not disclose these links to law enforcement agencies without consulting each of the affected organizations.

Where a referral is made to a law enforcement agency about such links, any subsequent exchange of information will occur bi-laterally between the law enforcement agency and the affected organization(s).

In the event links between participating private sector organizations are identified, each organization will be asked to confirm if its contact information, case reference number and the fact it may be affected by the same criminality as another organization(s) should be passed to the other organization(s).

On receipt of explicit confirmation to proceed IP Crime Unit staff will inform nominated representatives of each of the affected organizations that their information may have links with that submitted by another organization(s). Contact information and case reference numbers will be provided.

It should be remembered DIIP is a referral system which identifies common links between affected industries who are victimized by the same transnational organized criminals.

The extent to which INTERPOL tells affected organizations anything is: "Industry A, reference your case number ------ we think it is in your interests to speak to Industry B about their case/reference number ------" and visa versa.

Even then this will only take place if both industry A and B agree to this course of action and explicitly authorize INTERPOL to make the referral.

It is the industries themselves who decide if they wish to disclose their own information with similarly affected industries. That exchange takes place where the entities are located in the context of local national data protection regulations. (See: Data Handling and Referral Procedures – Section 6: Disclosure of Information and Referrals)

Q. Does INTERPOL publicize the names of affected organizations which provide information for the Database on International Intellectual Property (DIIP) Crime?

A. As a matter of principle INTERPOL will not publically disclose the identity of individual multinational industries or other participating entities that provide information for the Database on International Intellectual Property (DIIP) Crime without the explicit authority of the relevant industry or entity. This is to protect the confidentiality and proprietary interests of those entities that work with INTERPOL. It also protects the interests and neutrality of INTERPOL.

However, the names of cross-industry associations or representative bodies that contribute data to the Database on International Intellectual Property (DIIP) Crime may be disclosed with the explicit authority of the relevant association or body.

Q. What does INTERPOL do with the information it receives?

A. Information contained in DIIP will be subjected to criminal analysis to identify links between transnational and organized cross-industry sector IP criminal activity, facilitate criminal investigations, and develop regional and global strategic IP crime reports. (See: Data Handling and Referral Procedures – Section 5: Criminal Analysis)

Q. How effective is DIIP?

A. Comparisons between DIIP and ICIS to date indicate that for every 30 entities (e.g. names, addresses or telephone numbers) received from participating industries there is one hit on police information contained in ICIS. Hits have to be examined to establish if they are identical.

The fact there are hits shows there are links between transnational organized IP criminals known to police and participating industries. It also confirms the suspicion that transnational organized criminals who manipulate counterfeit and pirate goods also manipulate other illicit commodities and are involved in a wide range of other criminal activities.

This analysis illustrates the utility of DIIP, but for it to be truly effective and achieve its purpose there is a need to receive relevant information from all IP crime affected industries and subject it to systematic criminal analysis.

Q. How will the information be used to encourage policy makers in government and police forces to allocate more resources to combating transnational and organized IP crime?

A. INTERPOL will use criminal analysis to develop regional and global strategic IP crime reports. Strategic reports will neither contain nominal information nor proprietary information which could be used to identify an individual organization. Strategic reports will be used to illustrate the nature and extent of transnational organized IP crime and provide policy makers with an overview of counterfeiting and piracy. (See: Data Handling and Referral Procedures – Section 7: Strategic Reports)

Q. When a participating industry passes information to INTERPOL is ownership of the information transferred also?

A. No. The information always remains the property of the relevant participating industry. In accordance with INTERPOL Rules the owner of the information continues to have a duty to ensure the information is kept up to date

Q. How does a participating industry protect its interests and reduce any liabilities arising from providing information for DIIP?

A. INTERPOL has a duty to comply with its Rules on the Processing of Information for the Purposes of International Police Co-operation and the texts to which they refer. It is each industry's responsibility to ensure that it only shares relevant information with INTERPOL in accordance with national data protection requirements and its own data handling regulatory framework.

INTERPOL provides potential participating industries with a template letter of agreement which addresses these concerns. (See Appendix 3)

Q. Will DIIP be used to collect information from organizations other than participating industries?

A. DIIP will not be used to collect police information. Police information is submitted to INTERPOL through National Central Bureaus[6] in member countries.

INTERPOL is working closely with the public health sector under the auspices of the World Health Organization (WHO) International Medical Products Anti-Counterfeiting Task Force (IMPACT). The possibility of applying the DIIP model to the exchange of information between INTERPOL and the public health sector is being examined.

[6] INTERPOL has 186 member countries and each country has a National Central Bureau staffed by its own nationals. The NCB provides a gateway function for all official police interactions with the General Secretariat. Police information must be submitted through the relevant NCB.

Q. IP crime affected industries collect information in different ways and there is a lack of consistency. How does INTERPOL manage the transfer of information process?

A. It is recognized that industries collect information in different ways. INTERPOL will accept the information in any readily available electronic format (e.g. Access or XL). Information provided in a structured format can quickly be quality assured, organized and assimilated into DIIP.

Information received in report format without structure presents considerable difficulties because it is time consuming and expensive to assimilate and search it. Priority will be given to assimilating and processing structured information.

Q. Why has INTERPOL introduced the Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector?

A. Experience shows that some industries have invested heavily in combating counterfeiting and piracy. This includes the collection of information about transnational organized criminals. Other industries primarily collect information pertaining to core business with limited reference to transnational organized crime (e.g. limited information about customs seizures of counterfeit products bearing their trade mark).

INTERPOL has introduced the Recommended Minimum Global Standard to encourage all IP crime affected industries to collect searchable data about transnational organized criminal activity affecting their business which can be shared with INTERPOL and quickly assimilated into DIIP.

Q. Is the INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector mandatory?

A. No, it is a Recommended Minimum Global Standard which adds value to the collection of information about counterfeiting and piracy by affected industries.

Q. If industries do not adopt the Recommended Minimum Global Standard will INTERPOL decline to accept their submissions?

A. INTERPOL is an inclusive organization and will not exclude an IP crime affected industry from the process if it does not adopt the Recommended Minimum Global Standard. However, INTERPOL resources are finite and it is necessary to prioritize service delivery to stakeholders. Priority will be given to assimilating and processing structured information.

Q. How do I get more information about either the INTERPOL Database on International Intellectual Property (DIIP) Crime - Data Handling and Referral Procedures or the INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector?

A. Contact the INTERPOL IP Crime Unit at the following address:

Intellectual Property Rights Project
I.C.P.O. – INTERPOL
General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France

Tel : +33 4 72 44 57 95
Fax : +33 4 72 44 57 97

www.interpol.int

Appendix 2.

INTERPOL Database on International Intellectual Property (DIIP) Crime

Data Handling and Referral Procedures

1. **Introduction**

1.1. The INTERPOL Database on International Intellectual Property (DIIP) Crime is an autonomous INTERPOL iBase database containing information about transnational and organized intellectual property (IP) crimes.

1.2. Data contained in the database will be subjected to criminal analysis to identify links between transnational and organized cross-industry sector IP criminal activity; facilitate criminal investigations; and, develop regional and global strategic IP crime reports.

1.3. Police information is collected by INTERPOL in the usual way. It is forwarded to the General Secretariat through the appropriate National Central Bureau (NCB) and stored in the INTERPOL Criminal Information System (ICIS).

1.4. Non-police information is collected from participating private sector organizations and stored in the autonomous INTERPOL Database on International Intellectual Property (DIIP) Crime.

1.5. Information contained in the autonomous DIIP is compared to all police information contained in ICIS to identify links between IP crime and other types of criminality including drugs, firearms, fraud, money laundering, people trafficking, terrorism.

2. Control and Maintenance of DIIP

2.1. The INTERPOL IP Crime Unit (IPCU) is responsible for the control and maintenance of DIIP.

2.2. Access to DIIP is restricted to members of IPCU and nominated INTERPOL IT technicians responsible for database maintenance.

2.3. Participating private sector organizations that provide data do so on the understanding that to preserve confidentiality and protect the proprietary information of all contributors they will not have access to the data contained in DIIP.

3. Data Received from Participating Private Sector Organizations

3.1. Information received from participating private sector organizations should be provided in either the DIIP standard data format or in any readily available electronic format (e.g. Access or XL).

3.2. All data received from participating private sector organizations is quality assured by IPCU staff to ensure its accuracy, integrity, relevancy and status, including the review date before it is entered into the database.

3.3. Where appropriate and as part of the quality assurance process IPCU staff consult the owner of the information

3.4. Wherever possible to improve timeliness information received from participating private sector organizations will include the data fields contained in the INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector (Appendix 4).

3.5. In the event that the data is not provided in DIIP standard data format the data will be reviewed, prioritized and assimilated into DIIP by IPCU staff.

4. Comparison between DIIP and ICIS

4.1. IPCU staff systematically compare data in DIIP with police information in ICIS. It is undertaken in controlled circumstances. During the automatic comparison process the integrity of DIIP data is maintained. It is not stored in ICIS.

4.2. After the comparison has taken place IPCU staff carry out a detailed examination of all 'hits' to establish if they are confirmed links between DIIP data and the information contained in ICIS.

5. Criminal Analysis

5.1. IPCU staff conduct criminal analysis of DIIP data to establish if there are links between criminals, criminal organizations and affected participating private sector organizations.

5.2. IPCU produce intelligence packages about criminals and criminal organizations involved in transnational organized IP crime.

5.3. IPCU use the criminal intelligence to make informed decisions about the development of cross-industry IP crime law enforcement initiatives in INTERPOL Sub-regions in consultation with National Central Bureaus of participating countries.

6. Disclosure of Information and Referrals

6.1. In the event links between participating private sector organizations and other forms of ongoing criminality are identified IPCU does not disclose these links to law enforcement agencies without the express authority of each affected private sector organization.

6.2. Where a referral is made to a law enforcement agency about link(s) in 6.1. above, the exchange of information occurs bi-laterally between the law enforcement agency and the affected organization(s).

6.3. When links between participating private sector organizations are identified each organization is asked to confirm if its contact information, case reference number and the fact it may be affected by the same criminality as another organization(s) may be referred to the other organization(s).

6.4. On receipt of the necessary authority IPCU staff inform nominated representatives of each of the affected organizations that their information may have links with that submitted by another organization(s). Only contact information and case reference numbers are referred to the relevant organizations.

6.5. IPCU staff do not disclose the nature of the information. Bi-lateral discussions take place at the discretion of the parties concerned.

6.6. If asked, and it is appropriate to do so, IPCU staff will participate in bi-lateral discussions between affected parties

6.7. In the event IPCU identifies a major criminal conspiracy affecting a number of participating private sector organizations it may organize an operational working group meeting to enable affected organizations to identify a collective response to the identified criminality.

6.8. Subject to the Rules on the Processing of Information for the Purposes of International Police Co-operation and the texts to which they refer INTERPOL will not publically disclose the identity of individual multinational industries or other participating entities that provide information for the Database on International Intellectual Property (DIIP) Crime without the explicit authority of the relevant industry or entity. This is to protect the confidentiality and proprietary interests of those entities that work with INTERPOL.

6.9. Names of cross-industry associations or representative bodies that contribute data to the Database on International Intellectual Property (DIIP) Crime may be disclosed with the explicit authority of the relevant association or body

7. Strategic Reports

7.1. Criminal analysis is used to develop regional and global strategic IP crime reports.

7.2. Strategic reports do not contain nominal information.

7.3. Strategic reports do not contain proprietary information which could be used to identify an individual private sector organization.

7.4. Strategic reports are used to illustrate the nature and extent of transnational organized IP crime and provide policy makers with an overview of counterfeiting and piracy.

8. Performance Measurement

8.1. IPCU measure submissions received from participating private sector organizations for inclusion in DIIP.

8.2. IPCU measure the number and nature of possible links arising from comparison between DIIP data and ICIS

8.3. IPCU measure the number and nature of confirmed links arising from criminal analysis.

8.4. IPCU measure the number of intelligence packages produced.

8.5. IPCU measure the number of referrals made to participating private sector organizations.

Appendix 3

Database on International Intellectual Property (DIIP) Crime
Recommended Agreement Letter Template[7]

Intellectual Property Rights Project
I.C.P.O. – INTERPOL
General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France

Dear Sir

INTERPOL Database on International Intellectual Property (DIIP) Crime

Thank you for your invitation to participate in the INTERPOL Database on International Intellectual Property (DIIP) Crime.

We note that you are seeking the active participation and support of private sector organizations in order to develop and maintain a database that is used for the purposes of the detection and prevention of crime, and in particular, to identify links between transnational and organized cross-industry sector intellectual property criminal activity and to facilitate criminal investigations.

(Name of contributing entity) recognizes the need for industry to work in close cooperation with police, customs and other enforcement authorities in investigating and pursuing those engaged in intellectual property-related crimes and wishes to support INTERPOL's goals in relation to the DIIP.

Therefore, (Name of contributing entity) is willing to provide INTERPOL with information for the DIIP on the following bases:

1. INTERPOL presents its data requests to (Name of contributing entity) on a case by case basis in writing signed by an authorized person.

2. Each data request from INTERPOL outlines the particular information required with as much specificity as possible and explains the reasons why that information will assist INTERPOL in the prevention/detection of crime and the reasons why (Name of contributing entity)'s failure to provide the information may impede investigations.

3. Whether or not (Name of contributing entity) agrees to provide the requested information to INTERPOL in each case will be in (Name of contributing entity)'s

[7] The Recommended Agreement Letter Template is an example of a standard agreement between a participating industry entity and INTERPOL. It is accepted that a participating industry entity may add, delete or alter text to meet national legislation requirements.

sole discretion, taking into account (Name of contributing entity)'s data protection and confidentiality obligations.

4. Any information provided by (Name of contributing entity) to INTERPOL in response to a data request for the DIIP - the (Name of contributing entity) information – is provided by (Name of contributing entity) on an 'as is' basis as it exists at the time the information is extracted from (Name of contributing entity)'s records and (Name of contributing entity) makes no warranty as to its accuracy or completeness.

5. (Name of contributing entity) retains a duty to review and keep the information up to date in accordance with national data protection legislation. In the event (Name of contributing entity) becomes aware that particular information provided to INTERPOL contains a material error or omission and informs INTERPOL that the relevant information needs to be corrected or deleted or should not have been transmitted, INTERPOL will correct or delete the information accordingly.

6. INTERPOL will treat all (Name of contributing entity) information as confidential and in accordance with the procedures set out in the Database on International Intellectual Property (DIIP) Crime Data Handling and Referral Procedures forming Appendix 2 to the DIIP Consultation Document, dated 6 June 2008 (or procedures that are not substantially dissimilar to those procedures).

7. INTERPOL will immediately delete, destroy or return any (Name of contributing entity) information that is not necessary or subsequently becomes unnecessary for INTERPOL's crime detection and prevention purposes.

8. In the event that (Name of contributing entity) determines that an adequate level of protection is no longer being afforded by INTERPOL to the (Name of contributing entity) information, INTERPOL will, upon (Name of contributing entity)'s request, delete all (Name of contributing entity) information held in the DIIP.

Please confirm that the above terms are acceptable to INTERPOL by arranging for a duly authorized person to sign and return a copy of this letter to us.

Yours faithfully

Signed by a duly authorized person of (Name of contributing entity)

INTERPOL hereby confirms that it agrees to the terms and conditions set out above

Signed……..

Name……Position……

Date…….

Appendix 4

INTERPOL Database on International Intellectual Property (DIIP) Crime: Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector

Explanatory Note

The purpose of the INTERPOL Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector is to provide IP crime affected private sector entities with guidance about the type of information they should consider collecting about transnational and organized IP crime attacks on their interests.

It is expected that private sector entities will collect data about their business activities as a matter of course. However, the information collected for this purpose will not necessarily be information which can be used to identify if they are being attacked by the same organized criminals that are also attacking other entities or industry sectors.

Some private sector entities do systematically collect information about how transnational and organized IP criminals affect their business. Other private sector entities do not collect such information, but may wish to do so in the future.

The Recommended Minimum Global Standard provides both types of private sector entities with recommended minimum standards for the collection of information which is compatible with searchable information fields contained in the INTERPOL Database on International Intellectual Property (DIIP) Crime.

In the event that private sector entities adopt the Minimum Global Standard it will enable the information to be easily assimilated into the INTERPOL Database on International Intellectual Property (DIIP) Crime in accordance with DIIP Data Handling and Referral Procedures.

The Minimum Global Standard will also enable private sector entities to share information about transnational and organized IP crime with each other more effectively.

INTERPOL Database on International Intellectual Property (DIIP) Crime: Recommended Minimum Global Standard for the Collection of Information on Counterfeiting and Piracy by the Private Sector

DIIP Database Dictionary

Key: **Mandatory Field for completion by data contributors**
Desirable Field for completion by data contributors

INFORMATION OWNER	
Fields	***Format***
Information Originator Name	Text
Reference Number	Text and/or number
Country	Text
Address	Text
Phone Number	+33111111111
Fax Number	+33111111111
Email Address	Standard format
Website	Standard format

CONDITIONS	
Fields	***Format/Default***
Purpose	Prevention and detection of crime
Status	Confidential: to identify links between unrelated entities
Restrictions	For IPCU use only
Data Protection Review Date	DD/MM/YYYY

ACCOUNT	
Fields	***Format***
Account Number	Number
Name of Bank	Text
Sort Code	Number
IBAN Number	Number

ADDRESS	
Fields	***Format***
House Name/Street Number	Text/Number
Street Name	Text
City	Text
Country	Text
Post Code	Text/Number

COMMODITY	
Fields	***Format***
Property Type	Text
Seizure Date	DD/MM/YYYY
Seizure Country	Text
Quantity	Number

COMMUNICATIONS	
Fields	***Format***
Telephone Number & international code	+33111111111
Email	Standard format

ID DOCUMENT	
Fields	***Format***
Identity Document/Passport No.	Text and/or Number
Issuing Country	Text

ORGANIZATION	
Fields	***Format***
Name	Text
Company Registration No.	Number

PERSON	
Fields	***Format***
Forename	Free text
Surname	Free text
Sex	Male/Female/Unknown
Date of Birth	DD/MM/YYYY
Place of Birth	Text
Country of Birth	Text
Nationality	Text