Call for Interest for the INTERPOL Digital Crime Centre (CFI-12-IGCI-01)

Background

INTERPOL recognizes that police worldwide are facing an increasingly challenging operational landscape as criminals take advantage of new technology, the ease of international travel and the anonymity of doing business virtually. As criminal phenomena become more aggressive and elusive, notably in the area of cybercrime committed through the exploitation of technology, INTERPOL has embarked on a programme of innovation, which will see the opening of the INTERPOL Global Complex for Innovation (IGCI) in May 2014 in Singapore.

Complementing the General Secretariat Headquarters in Lyon, France, the purpose of the INTERPOL Global Complex for Innovation is to enhance INTERPOL's capability to tackle the crime threats of the 21st century and strengthen international policing worldwide.

The INTERPOL Digital Crime Centre will be the driving force of the Complex. Its activities will cover a range of areas essential to the assistance of national authorities: cybercrime investigation support, research and development in the area of digital crime, and digital security.

Two of the core elements of the Centre, and the subject of this Call for Interest, are the Digital Forensic Lab and the Cyber Fusion Centre.

Digital Forensic Lab:

The lab is expected to be a centre of excellence for forensic technology in the law enforcement community. The Lab has been allocated approximately 60-80m² in the Complex and is expected to be staffed by approximately 5 IT experts and investigators seconded from member countries and other external entities. It does not, however, aim to centre on academic research on cybercrime and cyber security; rather it will focus on practical technology that provides investigators with the capacity to better coordinate and conduct national and regional investigations.

The activities of the Lab can be broken down into 4 key areas which will, in conjunction with one another, provide the tools, intelligence and expertise required, as identified by law enforcement stakeholders themselves, to more effective combat cybercrime.

Trend Analysis

- The Lab will conduct strategic trend monitoring, and analysis of emerging crimes and threats to digital security through the employment of appropriate scientific methodologies.

- The Lab will engage strategic stakeholders, including the law enforcement community, research laboratories and institutions, academia, and the public and private sectors, to conceptualize and design state-of-the-art technological innovations that address current and future cybercriminal activities.

Testing Forensic Tools

- The Lab will identify, using Open Source Intelligence (OSInt) and partnership contacts, commercial and non-commercial Digital Forensic tools developed by private sector, academia and national level research laboratories.

- The Lab will drive, initiate and co-ordinate collaborative test-bedding of cutting edge IT tools, services and protocols that push the frontiers of cybercrime fighting and digital security, as well as advance the use of digital identity technologies and digital forensics.

Development of Best Practices

- The Lab will drive, initiate and coordinate collaborative research projects in innovative IT solutions with the view of improving digital-forensics capability and the use of digital identity technologies and other policing IT tools.

- The Lab will identify, develop and share Best Practices for cyber-incident preparedness and prevention as well as for incidence response activities.

- By using the results of the evaluation of digital forensic tools and techniques, and analytical reports regarding trend analysis, Standard Operating Procedure (SOP) for crime investigation shall be developed and shared with member countries.

Capacity Building and Training

- The Lab will develop and provide career development trainings for examiners, investigators and other first responders to ensure that they possess the latest knowledge of cybercrime trends, and the usage of digital forensic tools and techniques.

- The Lab will develop multi-level training modules/courses and materials with categorized core skill-sets and competencies for examiners and investigators.

- The Lab will operate a knowledge bank of modules/courses and materials to be accessed from member countries in order to facilitate information-sharing and maintain momentum of cyber security capacity-building.

<u>Cyber Fusion Centre</u>

The Fusion Centre will provide essential assistance to the Cybercrime Investigative Support (CIS) sub-directorate so that INTERPOL's member countries receive the intelligence and expertise required to effectively investigate cases of cybercrime.

The Fusion Centre will function in a manner similar to INTERPOL's Command and Coordination Centre, providing real-time monitoring of the network and analysis of malicious Internet activities. The Fusion Centre is expected to be housed in approximately 100-150m² and staffed by approximately 10 people.

The functions of the CFC will be divide into two complementary areas: Intelligence and Law Enforcement (L.E.) Action.

Intelligence

The Intelligence function of the Fusion Centre will be supported by personnel from Law Enforcement, Industry and Academia. The Intelligence function will:

- Conduct real-time analysis of threat feeds supplied by industry, package data, network activity, and other information and intelligence from open and friendly sources (such as IMPACT) in order to provide a holistic overview of malicious Internet activity, evaluate threats and action the information as needed.

- Generate analytical reports for member countries on the threats and actual problems identified in their countries to encourage discussion and multistakeholder efforts to improve the situation and thereby prevent crime.

- Produce an INTERPOL Cybercrime Treat Assessment or white papers from a the law enforcement perspective, which will identify cybercrime threats and encourage global action by pinpointing the cybercrime hotspots around the world.

- Supply relevant operational data to the L.E. Action personnel.

L.E. Action

Activities will be conducted by Law Enforcement personnel allowing for case-oriented analysis drawn from the Intelligence side of Fusion Centre to be turned into solid, intelligence driven identification of criminals.

- Consolidate criminal analysis of crime trends and turn this analysis into concrete operational action.

- Provide cybercrime expertise to national cybercrime units during investigations or coordinate cross border cybercrime investigations when there is not sufficient capacity.

- Deploy investigative support teams to assist national law enforcement agencies during investigations following a serious cybercrime incident.

Support Sought

INTERPOL has already identified some of the equipment, resources and information needed for the establishment and effective operation of the Lab and Fusion Centre. INTERPOL requests that interested parties take into consideration these requirements but also provide other additional proposals that will allow the Lab and/or Fusion Centre to fulfil its core activities. Identified items include:

Equipment and Tools

Contributions towards the furnishing of the DFL and CFC could be in-kind or purely financial.

- High specification computer workstations and servers
- Hardware and software for real-time monitoring and visualisation of network conditions, threat levels, incidents and network infections.
- Data storage and analysis facilities
- Licences and maintenance for Windows (XP, Vista or 7) and Virtual (VM) operating systems
- Licences and maintenance for essential word processing and analytical software packages
- Forensic tools, including: Encase, FTK, H/W & S/W type HDD Duplication devices,/tool, Sandbox or equivalent virus testing environment, mobile exploitation forensic tools
- Non-IT specific forensic tools: Video Surveillance/monitoring system, biometric devices (Facial, DNA, iris and other recognition)

Human Resource Support

- Software Examiners: duties would include malware and botnet analysis, testing of forensic tools, compilation of reports and development of best practices.

- Criminal Intelligence Analysts: trend analysis of cybercrime operandi and cyber security-related technology, and open source intelligence (suspects and incidences) collection.
- Technical Support: Assistance in configuring computers/networks/devices, trouble-shooting, and emergency response assistance when required.

Information and Intelligence Gathering

- Provision of cybercrime and security-related intelligence with regards to cybercrime and incidents; and emerging threats, including vulnerabilities and hot-fixes.
- Access to security-related data or databases: access to database storing raw packet data, and malicious packet collections for analytical purposes.

~~~~~~

INTERPOL invites interested companies and technological institutions to assist in the design, establishment, maintenance and partial-operation of the Digital Forensics Lab and/or Cyber Fusion Centre for a period of at least 3 years by providing technical equipment and tools, technical assistance and expert human resources[1].

INTERPOL is soliciting interested parties to produce their own proposals for the establishment of the Digital Forensics Lab and/or Cyber Fusion Centre, or to offer to collaborate on the creation of these functions with other interested parties.

INTERPOL will ultimately decide whether to select one company to assist in the design, establishment, maintenance and partial-operation of the Digital Forensic Lab and/or Cyber Fusion Centre, or to select a consortium of private sector companies and technological institutions to do so.

Call for Interest Objectives

INTERPOL announces a Call for Interest (CfI) to companies specializing in information technologies, as well as technological institutions, to obtain an indication of their interest to assist in the design, establishment, maintenance and partial-operation[2] of the Digital Forensic Lab and/or Cyber Fusion Centre in the INTERPOL Digital Crime Centre in Singapore by providing technical equipment and tools, technical assistance and expert human resources at no cost to INTERPOL for at least 3 years.

More specifically, any party interested to provide the abovementioned assistance for the Digital Forensic Lab and/or Cyber Fusion Centre to INTERPOL can opt to respond to the following two options:

1) By submitting your company, consortium or institution's interest to assist in the design, establishment, maintenance and partial-operation of the Digital Forensic Lab and/or Cyber Fusion Centre (*to be specified within the proposal*) as the sole vendor for the complete product by including your proposed concept functionalities, technologies, expertise, etc. and time for completion for the establishment of unit.

[1] Human Resources would be expected to be assigned linked to a Resources Assignment Agreement (RAA) unless otherwise agreed between INTERPOL and an interested party. RAAs may be concluded to obtain temporary additional human resources from institutions such as universities, private companies, foundations, law enforcement agencies and other national administrations. RAAs shall be concluded for a minimum duration of 2 weeks and a maximum of 12 months. The Organization shall not be responsible for emoluments, health insurance, welfare scheme and pension payments.

[2] Partial operation would refer to instances where any human resources might be detached from a private company to work in either the Lab and/or Fusion Centre.
~~~~~~

2) By agreeing to participate in the design and establishment of the Digital Forensic Lab and/or Cyber Fusion Centre containing specialized equipment or expertise from your company that could be incorporated in the Lab and/or Fusion Centre, founded with the assistance of one of the participating consortium companies.

Additional Conditions

a. Any interested company/institution or consortium thereof would be required to do all the design and development on its own and to absorb all costs related thereto.

b. Any interested company/institution or consortium thereof would be required to collaborate with the architects and interior design companies already contracted to design and build the INTERPOL Global Complex for Innovation. No modifications to structural design or layout would be permitted unless otherwise agreed with INTERPOL beforehand.

c. Any interested company/institution or consortium thereof would be required to provide installation and maintenance in Singapore, and provide an functioning product before the INTERPOL Global Complex for Innovation becomes operation in May 2014.

d. Following the acceptance of a party's proposal, INTERPOL can be consulted to give input along the way to review draft designs of the Lab and/or Fusion Centre.

e. Prior to entering into an agreement, any interested company/institution or consortium thereof would be required to have all key Officers and Board Member to be subject to national and INTERPOL background checks. INTERPOL reserves the right to apply other due diligence procedures prior to entering into a commercial agreement.

CALL FOR INTEREST
INTERPOL Digital Crime Centre
–
ADDITIONAL INFORMATION

1. CONDITIONS OF THE CALL FOR INTEREST

Modification or cancellation of the call for interest

INTERPOL is not bound to take any further action with any party as a result of this Call for Interest. It reserves the right, at all times and at its entire discretion, without having to justify its decision, to ask for a change in the goods, works and/or services or communicate to applicants any modifications or corrections to the information relating to its needs.

Any modifications/corrections of the needs will be notified directly to all the applicants that have submitted an application in the framework of the present Call for Interest.

Should any changes occur within five (5) working days before the deadline for the submission of the applications, INTERPOL reserves itself the right to extend the deadline to allow sufficient time for applicants to respond depending on the importance of the modifications/corrections. The fact that INTERPOL decides not to extend the deadline does not entitle applicants to claim any compensation or to any form of complain whatsoever.

Confidentiality

All information, regardless of its medium, sent to applicants or which applicants may access for the call for interest hereof, other than information displayed on INTERPOL public website is confidential and may not be used for any purposes other than the submission of an application. INTERPOL reserves the right to retrieve this information at the end of the Call for Interest.

Discussions

INTERPOL reserves the right to discuss with the applicants, without these discussions being considered, in any way whatsoever, as a desire to conclude the transaction with the applicants. With respect to this and until the effective signing of an agreement, INTERPOL is entitled to stop any negotiations. This suspension of discussions shall not, under any circumstances, entitle the applicants to claim any compensation.

INTERPOL shall give details of this stage in due time directly to the candidates who have expressed their interest. These presentations may either take place at the INTERPOL's headquarters or via videoconference.

INTERPOL also reserves the right to conduct on-site visits.

Compensation

INTERPOL does not foresee to compensate applicants in any way or for any reason whatsoever with respect to the present Call for Interest.

2. SUBMISSION CONDITIONS

All responses to this Call for Interest must be made by completing the attached Letter of Interest and sending it to cfi.digitalcrime@interpol.int with "*INTERPOL Digital Crime Centre, CFI - Letter of Interest*" in the subject heading.

All questions may be sent by e-mail to ao-ab-adm-pcm@interpol.int with "*INTERPOL Digital Crime Centre, CFI - Questions*" in the subject heading until **31 August 2012 at 17h00** (Paris time). INTERPOL reserves the right to respond to questions deemed relevant to the Call for Interest and to share the responses with other candidates, if it considers the information useful for other candidates.

Prototypes and/or additional technical documentation as specified in each chosen option can be sent to the below address. All submissions must be received on or before **12 September 2012 at 17h00** (Paris time) and become the property of I.C.P.O. – INTERPOL. This Letter of Interest is not binding.

3. CONTENT OF YOUR SUBMISSION

The submission shall at the minimum contain the following information:

- the Letter for Interest (as many letters of interest as members of the consortium);
- the questionnaire with supporting documents as requested in the questionnaire;
- the project outline;
- a signed and dated copy of the present document.

In addition, you may submit additional material such as a prototype or commercial brochures that you feel substantiate your submission, and particularly any statement related to performance it contains. Documentation can be sent via e-mail at the e-mail addresses cfi.digitalcrime@interpol.int. Messages sent to this e-mail address shall not be viewed before the deadline of 12 September 2012.

Please note that the messages may not exceed the volume of **10Mo.** In case of need, the submission may be sent in several messages.

Submissions must be written in English.

Letters of Interest, questionnaires as well as project outlines supplied in response to this Call for Interest are likely to be made available to INTERPOL member countries during the Organization's General Assembly. Accompanying documentation may also be made available to member countries. With the exception of the project outline, any other information that is considered non-disclosable to all member countries should be identified as such. Non-disclosable information will be retained exclusively for the use of the staff of the General Secretariat in charge of analysis of the submissions.

Read and approved:

Date:

Name and position of signatory:

Letter for Interest concerning the Call for Interest for the INTERPOL Digital Crime Centre (CFI-12-IGCI-01)

Name of Organization:	
Name and function:	
Address:	
Telephone:	
Fax:	
E-mail:	

I express my interest in the INTERPOL Digital Crime Centre in response to INTERPOL Call for Interest (CFI-12-IGCI-01), concerning the following option(s) (check all that apply):

1. ☐ by submitting your company, consortium or institution's interest to assist in the design, establishment, maintenance and partial-operation of the Digital Forensic Lab and/or Cyber Fusion Centre (*to be specified within the proposal*) as the sole vendor for the complete product by including your proposed concept functionalities, technologies, expertise, etc. and time for completion for the establishment of unit.

2. ☐ by agreeing to participate in the design and establishment of the Digital Forensic Lab and/or Cyber Fusion Centre containing specialized equipment or expertise from your company that could be incorporated in the Lab and/or Fusion Centre, founded with the assistance of one of the participating consortium companies.

N.B. *All submissions, including this Letter of Interest, exemplars and/or technical documentation should be received before 17:00 (Paris time),* ***12 September 2012****.*

ADDITIONAL QUESTIONS

TECHNICAL PROPOSAL

1. Does the solution your company proposes cover the full scope of the project?

☐ YES ☐ NO

2. If you answered NO to question 1, please specify which specific feature you propose to develop.

_____
_____
_____
_____

3. As indicated in the call for interest announcement, supporting information and brochure may be provided as part of your response. However, your response **must** contain a project outline (maximum 3 pages).

FINANCIAL PROPOSAL

4. Would you be in a position to offer your solution at no costs whatsoever to INTERPOL and this for at least 3 years starting from the delivery of the solution to INTERPOL?

☐ YES ☐ NO

YOUR PARTNERS

5. Please indicate

if you intend to set up a consortium to propose the full solution? and/or

☐ YES ☐ NO

if you agree to take part in a consortium that would already be set up by another company?

☐ YES ☐ NO

6. If you intend to deliver your solution via a consortium, thank you for giving in a separate sheet the following information:

    a) Composition of the consortium and explain how it is suitable to the objectives of the project. Please indicate the entity that will serve as INTERPOL's contact point.
    b) If the consortium is already set up, specify responsibilities within the consortium.
    c) For each member of the consortium, please submit a filled in letter for interest as well as all information required in points 8 and 9.
    d) For each member of the consortium, please indicate the main tasks they have been attributed and the previous experience relevant to those tasks.
    e) If applicable, please provide material concerning projects that have been or currently are conducted by the same consortium.
    f) Are there roles yet to be assigned? If so, please specify which one(s).

BACKGROUND EXPERIENCE

7. Please give evidence of projects of a similar nature you have conducted or are currently conducting. INTERPOL is particularly interested in the scope, costs and timeframe of such projects. For each project, please indicate a person INTERPOL could contact for further details.

LEGAL AND ADMINISTRATIVE INFORMATION

8. In order to assess your proposal, we wish to receive the following financial and administrative information about your company:

a) Legal status

b) Fiscal status

□ Company or association subject to company tax. Pays this tax itself.
□ Member of group for which company tax is paid by the parent company.
Name or corporate name of parent company:
□ Individual company or EURL (one-person limited company) subject to income tax.
□ Company consisting of individuals or an economic interest grouping comprising the following natural persons or legal entities, themselves liable to income tax (IR) or company tax (IS) proportionate to their share of the profits:

c) Registration

□ Registration No.: …….

□ Commercial register, number and town of registration
(Append a copy of the official company registration document giving the company details; the copy should be marked "Administrative information – Item 8.c")

□ Trades register, number and office where registered:
Reason for not giving a commercial registration number or trades register

□ The applicant is a natural person not engaged in commercial activity and is not required to be listed in the business and companies register (RCS) or on the trades register. If the profession of

which he/she is a member is subject to specific regulations, please give below the details of registration with a professional body or of the consent given by the competent authority.

□ Company set up on:
……
Registration request submitted to the following body (designation and address):

□ Registered association set up on: …….
(Append a copy of an official document issued by the competent national authority giving the reasons for this situation; the copy should be marked "Declaration by candidate – Item 8")

d) Authorized company signatories (name and position)

e) Financial information:

Authorized capital (if applicable) in euros**:**

Post-tax turnover for the last three full tax years (in euros):

f) Is your company subject to a compulsory winding up order (or an equivalent foreign procedure)?

□ No □ Yes

If yes: Attach the relevant legal document, marking it "Administrative Information – Item 8.f**'**. (If not in English, this must be accompanied by a certified translation.)

g) Resources

Technical equipment and research resources, human and material resources likely to be deployed if selected.
(Attach details, marking it “Administrative Information – Item No. 8.g")

h) Other documents to be attached

(Please attach the following documents, marking them “Administrative Information” – Item No. 8.h")

• Official document issued by the competent national authority certifying that the company is up to date with its social insurance contributions

• Civil liability insurance certificate (ten-year cover if appropriate in the light of the subject of the Transaction) giving details of the type of cover, the amounts guaranteed and excess per claim

• Security clearances, widely acknowledged professional qualifications or labels (such as ISO…)

• Other documents to be attached, as further indicated in the call for interest documents.

9. Please provide on a separate sheet, the following certificates:

a) The Candidate's authorized signatory certifies that neither he/she, nor the company and those holding positions is in a state of liquidation of assets or personal bankruptcy or is subject to equivalent procedures (if the bidder is located abroad), that the company has not been prohibited from doing business on free and fair competition according to national and international laws and regulations and that it has fulfilled its fiscal and employer's obligations.

b) The Candidate's authorized signatory declares that the work will be carried out with due regard for relevant national and international legislation.

c) The Candidate’s authorized signatory declares that its activities are compatible with the principles, aims and activities of INTERPOL, as set out in particular in INTERPOL’s Constitution.

I hereby certify information contained in this document is accurate and that the documents submitted are certified copies of the originals:

Date:
Name and position of signatory:

When information is to be supplied on a separate sheet, applicants may submit them in a single document, provided clear reference to the questions concerned is given.