EOI Invitation to Content Developers for Training in area of Cyber Crime Investigation and Digital Forensics for National Cybercrime Training Centre(N.C.T.C.) under Indian Cyber Crime Coordination Centre (I4C) Scheme of Govt. of India

National Crime Records Bureau
Ministry of Home Affairs
Government of India

April, 2019

Table of Contents

1. Introduction

Cybercrime is becoming a global phenomenon and a worldwide concern. As Cyber criminals face no boundaries, the traditional law enforcement approach is becoming obsolete. If the borders and artificial boundaries set up by countries are becoming a big obstacle to investigate and prosecute traditional crime, the concerns are even bigger in regards to identifying, investigating, prosecuting and bringing cyber criminals before justice.

Indian Cybercrime Coordination Centre (I4C) aims to overcome obstacles by assisting state law enforcement agencies in all aspects regarding cybercrime intelligence development and sharing, training, forensics, research, and also by facilitating exchange of information and cooperation amongst them. A vital aspect for fighting cybercrime is that the state law enforcement agencies have cyber intelligence, investigation and forensic units that are fully prepared both from the equipment and the knowledge point of view to face Cyber criminals and their destructive actions.

Cybercrimes have been divided broadly under three heads:

a. Pure Cybercrimes

i. Ransomware
ii. Hacking
iii. Distributed Denial-of-Service (DDOS) Attacks
iv. ATM Malware
v. Attacks on Financial Infrastructure (like SWIFT infrastructure)
vi. Bitcoin Thefts
vii. Theft of Computational Resources
viii. DNM (Dark Net Market) Exit Scams

b. Cyber Enabled Crime

i. Frauds / Cheating
ii. Lottery Scams
iii. Business Email Compromise
iv. Money Laundering
v. Social Media Harassment

c. Incidental Cybercrime

Use of some amount of cyber space (including Digital Devices) is incidental for commission of crimes / presence of evidence / presence of victims / presence of suspects — this covers practically all crimes.

2. Implementation Plan

National Cybercrime Training Centre (NCTC) has been entrusted under I4C to establish a Massive Open Online Platform (MOOC) for facilitating training and certification on Cyber Crime Investigation and Digital Forensics. In order to provide these course on MOOC platform it is envisaged to get content developed by some reputed organization/firm/joint venture who would be also be responsible for designing the standard module training curriculum, including identification of roles and required skill sets, standardization & certification mechanism. Cyber Range or Simulated Cybercrime Scenarios are the key component of such a training model. Besides preparation of traditional modes of training through books, boards, power point/PDF-based approach, there is a strong need for more trainings based on simulated environments. This would mean creation of scenarios, including digital exhibits (logs, etc.) for extraction by trainees using forensic tools preloaded on the infrastructure, using appropriate procedures. The firm/organization/joint venture will also be involved in continuous upgradation of course curriculum on cybercrime investigation.

3. Purpose of EOI

The purpose of this Expression of Interest (EOI) is to identify content developers who can develop content in area of Cyber Crime Investigation and Digital Forensics including simulation based training for National Cybercrime Training Centre(N.C.T.C.) under Indian Cyber Crime Coordination Centre (I4C). The objective of the document is to provide indicative information on the envisaged modular training structure and the scope of work for this project. The detailed scope of work, terms and conditions and parameters for selection of the content developer may be provided in the form a Request for Proposal (RFP) after consultation with the possible Content Developers applying to this EOI.

4. Timelines

a) NCRB invites expression of interest from organizations who meet the eligibility criteria as stated under Section - Eligibility Criteria with all the necessary documents in a sealed cover along with the covering letter duly signed by an authorized signatory at the below address:

   Joint Director(CCTNS)
   National Crime Records Bureau
   NH-8, Mahipalpur
   New Delhi-110037

b) The Expression of Interest may be submitted before 31.05.2019 Any EOI received after the cut-off date and time will be rejected.

c) Soft copy of the EoI Proposals should also be submitted over email at nctc@ncrb.nic.in as per timelines already provided above.

d) Any queries related with this EOI should be mailed at nctc@ncrb.nic.in by 28.05.2019

e) Consultative Meeting :- NCRB shall hold a pre-bid meeting with the prospective Content Developers at :

National Crime Records Bureau
NH-8, Mahipalpur New Delhi-110037

5. Scope of Work

The broad scope of work as part of this EOI form is as given below:

5.1. Designing the Training Curriculum

The training curriculum has to be designed with a broad general awareness package and followed by capacity building under two broad heads i.e.

a) Training Tracks

b) Awareness Tracks

Training Tracks are

i. Responders Track

ii. Digital Forensics Track

iii. Investigations Track and

iv. Intelligence Track

Awareness Tracks are

I. Management Track

II. Judiciary / Prosecution Track

These training tracks can further be divided in to Fundamental, Intermediate and Advance levels. Initially following roles and curriculum has been developed for each track including the simulations facilitating learners opportunity to do hands-on

1. Responders Track

This course is meant for First Responder Officer who can be a PCR Van officer or the Emergency Officer of the Jurisdictional Police Station. He is often the first to arrive on the scene of crime and needs to have an awareness of how technology affects crime, what is digital evidence and

how it should be handled and Duty Officer who is the Frontline officer that receives and offers first line response to complaints involving crime using technology. He/She needs to assess complaints and respond appropriately to instances of crime using technology and make appropriate referrals where required and/or necessary.

The proposed contents of the course are

a) Fundamentals

- General Cybercrime Awareness; Crime Scene Attendance ;Understanding Digital Evidence

b) Intermediate

- Cyber legislation concepts ;Risks of cyber investigations

c) Advanced

- Jurisdiction specific SOP; Awareness on new trends in technology

2. Digital Forensics Track

This course is meant for Digital Forensics Specialist whose main job of a Digital Forensics Specialist is to perform recovery and investigation of material found in digital devices. The Digital Forensics Specialist has a technical background and has to be able to apply knowledge of computer forensic principles in the identification and collection of digital evidence.

The proposed content of the course are

a) Fundamentals

- Introductory Open Source IT Forensics; Core Mobile Phone Forensics ; Basic Commercial Tools Training ;Windows Forensics(NTFS)

b) Intermediate

- Live Data Forensics; Intermediate Network Forensics; Intermediate Mobile Phone Forensics ; Linux as an Investigative Tool ; Introduction to Malware Analysis

c) Advanced

- Forensic Scripting; Advanced Malware Analysis; Cloud forensics ; Cryptocurrencies forensics; IOT devices; Advanced Mobile Forensic Techniques: JTAG and Chip-off Forensics; Decryption; Audio/Video Forensics; Advanced Commercial Tools Training

3. Investigations Track

This course is meant for General Investigator who is a police officer that handles criminal cases in a wide variety of police operational units. This investigator handles increasingly more technological related issues regarding the cases that he is required to solve and needs good Cybercrime and Digital Forensics awareness skills.

The proposed contents of the course are

a) Fundamentals

- General Cybercrime Awareness and types of cybercrimes; Network Investigations Fundamentals; Internet Investigation Fundamentals; Cybercrime legal issues

b) Intermediate

- Internet investigations; Network Investigations; Linux as an Investigative Tool, part 1; Social media and Open Source Intelligence (OSINT)

c) Advanced

- Linux as an Investigative Tool, part 2; Deep web and Virtual Currencies Simulation Training; Wireless LAN & VOIP Investigations; DNS abuse and criminal use of DNS

4. Intelligence Track

The course is meant for Cybercrime Intelligence Officers/Analysts are identifying and producing intelligence on Cybercrime from raw information; assembling and analyzing multi-source operational intelligence; preparing and presenting intelligence briefings; preparing planning materials for photographic reconnaissance missions; analyzing the results, preparing reports. They are required to prepare graphics, overlays and photo/map composites; plotting imagery data using maps and charts; providing input to and receive data from computerized intelligence systems; maintaining intelligence databases, libraries and files.

The proposed content of the course are

a) Fundamentals

- General Cybercrime Awareness; Strategic and operational crime analysis

b) Intermediate

- Analytical and visualization tools; Network Investigations Fundamentals; Social media and Open Source Intelligence (OSINT); Big data management and analysis

c) Advanced

Databases and data mining

5. **Management Track**

This course is meant for Cybercrime / Digital Forensics Head of Unit (SP / DCP): These professionals deal directly with cyber investigators and experts. They should take informed decisions in cybercrime cases or in other complex investigations involving cybercrime elements. Their role is to coordinate staff, allocate resources and prioritize policing activities. They should have detailed overview of the capacity, capabilities and needs of the unit and provide it with the relevant training and tools that enable or facilitate investigation and examination of the evidence. Another function is to represent the unit when dealing with external stakeholders. They need at least a minimum of hands-on practical experience to evaluate operational and strategic activities and the ability to communicate effectively with their staff and external experts. Additionally this course is also meant for Heads of Police Forces (DGP) who are the Law Enforcement Managers, who are responsible for creating and executing strategic initiatives to increase efficiency of policing activities while dealing with obstacles such as legislation changes or staff turnover. They influence key external stakeholders and promote the organization in the media. They establish policies and procedures for the organization to allocate available resources. This group should benefit from advanced awareness on Cybercrime. The actors should be able to maintain an effective working relationship with the head of the Cybercrime unit and represent cybercrime policing in the media. At a general level, the Cyber related threats, legislation, opportunities and limitations must be understood.

The proposed content of the course are

a) Fundamentals

- General Cybercrime Awareness and types of Cybercrimes; Cybercrime legal issues; Managing a Cybercrime/Digital Forensics Unit; Network Investigation Fundamentals

b) Intermediate

- Managing a Cybercrime/Digital Forensics Unit; Managing an international cyber investigation; Internet investigation ; Network Investigation

c) Advanced

- Social media and Open Source Intelligence (OSINT)

6. Judiciary / Prosecutors Track

This course is meant for Judges / Prosecutors who handle a wide variety of criminal cases. They should get an awareness of how crime can be facilitated by technology and what digital evidence is and how it can be used in a case. Additionally it also meant for Specialized Cybercrime Judge/Prosecutors are specialized in prosecuting/judging technology enabled crime cases or specifically Cybercrime cases.

The proposed content of the course are

a) Fundamentals

- General Cybercrime Awareness and types of cybercrimes; Cybercrime legal issues; Network Investigation Fundamentals

b) Intermediate

- Internet investigations; Network Investigations; Social media and Open Source Intelligence (OSINT)

7. General Awareness Package on Cybercrime Investigations and Digital Forensics

Apart from the above a generalized curriculum has also been identified which will be placed in various curriculums depending on the need which is name as **General Awareness Package on Cybercrime Investigations and Digital Forensics**

This module is intended to introduce basic concepts on the following topics:

a) Cybercrime Investigations:

- General Cybercrime awareness including types of cybercrimes and other tech enabled crimes.
- Internet basics - URL, DNS, Domain names and IP addresses ISPs.
- Email investigations and other communication technologies.
- Proxies and Anonymous Investigations
- Social media and Open Source Intelligence (OSINT)
- Social Engineering
- Deep Web and Anonymization techniques
- Virtual Currencies Concepts

b) Digital Forensics:

- Digital Evidence
- Digital crime scene examination skills including seizing of electronic evidence, chain of custody and presenting evidence in court.
- Crime Scene Attendance
- Introduction to Malware Concepts
- Preservation of Digital Evidence
- Mobile Applications

c)Legal issues when handling digital evidence or performing online investigations:

- Fundamental knowledge of legal and jurisdiction issues (may include reference to Country's Legislation and obligations under International Treaties)
- How to present evidence in court
- Requesting and processing subscriber information and data from third parties
- Cyber legislation concepts

Risks of cyber investigations

5.2. Prepare Standardized Content

For each of the above track elearning material has to be developed which will be loaded on a Massive Open Online Course(MOOC) Platform which has been created for online personalised, interactive or virtual education. The material available on **UNODC Global eLearning Platform** and **INTERPOL Global Learning Centre (IGLC) are** examples in this area.

5.3. Standardisation and Certification Method

There is a strong need for a standardized nationally recognized certification in fighting Cybercrime. NCTC will be uniquely placed to provide such a certification mechanism. A large majority of the Digital Forensics specialists and Cybercrime investigators are required to testify in court and so they are constantly being challenged on the basis of their certifications and professional knowledge. There has been a strong need to setup a standardized certification that can be nationally accepted, recognized and which can be presented in courts to further testify for the strong Cybercrime investigations, or Digital Forensics knowledge of the holder.

NCTC aims to setup such a certification system, based on the proposed training system described above. This training curriculum will provide law enforcement officers with two certifications:

- Specialist
- Certified Expert

6. EOI Proposal Preparation Costs & related issues

a) The vendor is responsible for all costs incurred in connection with the participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/presentations, and preparation of EOI along with providing any additional information required by NCRB.

NCRB will in no case be responsible or liable for those costs, regardless of the conduct or outcome of this EOI.

b) This EOI does not commit NCRB to award a contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award or for preparing this EOI.

c) All materials submitted by the vendor will become the property of NCRB and may be returned completely at its sole discretion.

7. Eligibility Criteria

Mandatory Eligibility Criteria are as below:

a) Legal entity recognized under law: The interested firm/Organisation/Joint Venture should be a legal entity recognized under Indian laws and in case of a foreign company, should be registered under the laws of such foreign country and authorized to participate in Government of India bidding process by the competent authority in India.

b) Financial turnover: The Annual Business turnover should be minimum of Ten(10) Crores for last three financial years while working in similar / related projects. Relevant document to be submitted along with the EOI.

c) Positive Net Worth - The Bidder shall have a positive net worth in each of the following years 2016-2017, 2017 – 2018 and 2018-2019.

d) Incorporation: The said legal entity should have been in existence for a period of at least 2 years on the date of submission of proposal as evidenced by the documents submitted by such entity in its proposal.

e) Expertise: The firm/organisation/joint venture should have experience and proven track record of having conducted similar projects related to designing the standardised modular training curriculum including certification, upgradation of

course curriculum on Cybercrime. A statement of work done or such projects undertaken need to be submitted

f) **Blacklisting:** The firm/Organisation/Joint Venture should not be blacklisted by any Central Govt. / State Govt. / PSU/Govt. bodies/ any foreign organisation. Undertaking Certificate signed by the Authorized signatory should be submitted along with the EOI.

Additional Desired but not limiting Criteria are as below:

a) **Quality Management Certification:** The firm/Organisation/Joint Venture should have ISO 9001 certification as on the date of submission of response and a copy of certificate valid on the date of submission of the EOI response should be submitted.

b) **Information Security Management Certification:** The firm/Organisation/Joint Venture should have ISO 27001 certification as on the date of submission of response and a copy of certificate valid on the date of submission of the EOI response should be submitted.

8. Right to Terminate the Process

NCRB may terminate the EOI process at any time and without assigning any reason. NCRB makes no commitments, express or implied that this process will result in a business transaction with anyone. This EOI does not constitute an offer by NCRB

9. Submission of EOI

All Original Cybercrime Training Content Developers are invited to submit an EOI to National Crime Records Bureau.

I. The scanned versions of the documents or pdf versions of the following documents need to be submitted:

Form 1: Covering Letter with Correspondence Details

Form2: Details of the Bidder's Operations and Cybercrime Training Content development

Form 3: Compliance Sheet for Eligibility Criteria

Form 4: Financial Information (as per Audited Balance Sheets)

Form 5: Capability Citation Format

Form 6: Format to indicate no Blacklisting

Form 7: Proposed Implementation Plan

*Formats for these forms are given under **Annexure – I***

Additional:

(a) Power of Attorney in the name of Authorized Signatory

(b) Documents requested in the Section 7 – Eligibility Criteria of this EOI document

10. Assessment Process:

a) NCRB will constitute an Evaluation Committee to evaluate the responses of the applicants.

b) For the submitted EOIs meeting eligibility criteria as stated under section 4, Initial shortlisting will be done based on their past experience of handling similar type of project. Shortlisted organizations will be invited for presentation in front of Assessment Committee.

c) The Assessment Committee constituted by NCRB shall evaluate the responses to the EOI and all supporting documents & documentary evidence. The committee may seek additional documents / presentation as it deems necessary.

11. Appendix I - Bid Submission Forms

Form 1: Covering Letter with Correspondence Details

<Location, Date>

To

Joint Director(CCTNS)

National Crime Records Bureau

NH-8, Mahipalpur

New Delhi-110037

Dear Sir,

We, the undersigned, offer to provide the Content Developer Services **for standardized modular training structure with training methodology for LEAs using simulated environment for National Cybercrime Training Centre(N.C.T.C.)**

Our correspondence details with regard to this EoI are:

S. No.	Information	Details
1	Name of the Contact Person	<Insert Name of Contact>
2	Address of the Contact Person	<Insert Address>
3	Name, designation and contact, address of the person to whom, all references shall be made, regarding this EOI	<Insert Name of Contact>
4	Telephone number of the Contact Person.	<Insert Phone No.>
5	Mobile number of the Contact Person	<Insert Mobile No.>
6	Fax number of the Contact Person	<Insert Fax No.>
7	Email ID of the Contact Person	<Insert Email>
8	Corporate website URL	<Insert Website URL.>

We are hereby submitting our Expression of Interest. We understand you are not bound to accept any Proposal you receive. We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading the short-listing process or unduly favours our company in the short-listing process, we are liable to be dismissed from the selection process or termination of the contract during the project.

We hereby declare that our proposal submitted in response to this EOI is made in good faith and the information contained is true and correct to the best of our knowledge and belief.

Yours Sincerely,

[Company Name with seal]

<Applicant's Name with seal>

Name: <<Insert Name of Contact>>

Title: <<Insert Title of Contact>> Signature: <<Insert Signature>>

Form 2: Details of the Bidder's Operations for Cybercrime Training Content development

S. No.	Information	Details to be furnished
1	Name and address of the bidding Company	
2	Incorporation status of the firm (public limited / private limited, etc.)	
3	Year of Establishment	
4	Date of registration	
5	ROC Reference No.	
6	Details of company registration	
7	Details of registration with appropriate authorities for service tax	
8	Name, Address, email, Phone nos. and Mobile	

[Company Name with seal]

<Applicant's Name with seal>

Name: <<Insert Name of Contact>>

Title: <<Insert Title of Contact>>

Signature: <<Insert Signature>>

Form 3: Compliance Sheet for Eligibility Criteria

S. No.	Basic Requirement	Required	Provided	Reference & Page Number
1	Power of Attorney	Copy of Power of Attorney in the name of the Authorized signatory	Yes/No	
2	Covering Letter with correspondence details	As per given "FORM 1: Covering Letter with Correspondence Details" in this Appendix.	Yes/No	
3	Legal Entity	Copy of Certificate of Incorporation; and Copy of Service Tax Registration Certificate	Yes/No	
4	Annual Sales Turnover	Certificate from the statutory auditor or by Company Secretary, along with the Balance Sheets of the last three financial years which are available publicly (Form 4)	Yes/No	
5	Net Worth		Yes/No	
6	Technical Capability	Certification by Company Secretary of having delivered Similar project(s) and of project(s) Gone-Live (Form 5)	Yes/No	
7	Standardisation & Certification	Copy of certificate	Yes/No	
8	Quality Management Certification	Copy of certificate	Yes/No	
9	Information Security Management Certification	Copy of certificate	Yes/No	
10	Blacklisting	Certificate by authorized signatory (Form 7)	Yes/No	

[Company Name with seal]

<Applicant's Name with seal>

Name: <<Insert Name of Contact>>

Title: <<Insert Title of Contact>>

Signature: <<Insert Signature>>

Form 4: Financial Information (as per Audited Balance Sheets)

	2016-17	2017-18	2018-19
Annual Sales Turnover (in Crores)			
Net worth (in Crores)			
Other Relevant Information			

The copies of respective balance sheets are enclosed.

*It is confirmed that I am/we are the statutory auditors / Company Secretary of M/s

_____

_____

< Statutory Auditor/ Company Secretary's Name with seal>

<Signature of Statutory Auditor/ Company Secretary> Name:

Date & Place:

Note: The above certificate should be from the statutory auditor or Company Secretary of the bidder organization.

* Strike out whichever is not applicable

Form 5: Capability Citation Format

Relevant project experience needs to be mentioned (provide no more than 3 projects)

Project 1/2/3

General Information	
Name of the project	*Provide reason in case information is being withheld*
Client for which the project was executed	*Provide reason in case information is being withheld*
Name and contact details of the client	*Provide reason in case information is being withheld*
Confirmation of project delivery and Go Live	**"It is hereby certified that the cited project has been delivered and gone live"**
Project Details	
Description of the project covering the following :- 1. Broad scope of Work 2. Cybercrime Training Content Development 3. Standardisation & Certification methods used 4. Outcomes of the project	You are encouraged to provide as much information as possible to allow assessment Work order/ documentary evidence be provided if NDA is not an issue
Other Details	
Total cost of project for which Purchase order has been placed on vendor (in INR)	
Start Date of the Project	
Go live Date of the Project	
Target Completion date of Project	
Project Status (Completed/ Maintenance)	
Other Relevant Information	
Letter from the client to indicate the award of work/ successful completion of the project	*Optional. Indicate page number, in case attached.*

Note: If any information provided by the vendor by way of self-certification or otherwise is found to be false, the vendor would be disqualified at any stage.

[Bidder's Name with seal]

<Applicant's Name with seal>	<Company Secretary's Name with seal>
Name: <<Insert Name of Contact>>	Name: <<Insert Name of Contact>>
Title: <<Insert Title of Contact>>	Title: <<Insert Title of Contact>>
Signature: <<Insert Signature>>	Signature: <<Insert Signature>>

Form 6: Format to indicate no Blacklisting

In response to the EOI dated _____ from **Content Developers for Training in area of Cyber Crime Investigation and Digital Forensics for National Cybercrime Training Centre(N.C.T.C.) under Indian Cyber Crime Coordination Centre (I4C) Scheme of Govt. of India,** I/We hereby declare that presently our Company/ Firm _____is having unblemished record and is not declared ineligible for corrupt & fraudulent practices either indefinitely or for a particular period of time by any State/ Central Government/ PSU/Autonomous Body.

I/We further declare that presently our Company/ firm _____is not blacklisted and not declared ineligible for reasons of corrupt & fraudulent practices by any State/ Central Government/ PSU/ Autonomous Body on the date of EOI Submission.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, our EOI to the extent accepted (if any) may be cancelled.

Bidder's Name with seal]

<Applicant's Name with seal>

Name: <<Insert Name of Contact>>

Title: <<Insert Title of Contact>>

Signature: <<Insert Signature>>

Form 7: Proposed Implementation Plan

A comprehensive proposed implementation plan along with approach and methodology as described in Broad Scope of work in this EOI should include various activities such as designing the standardized modular training curriculum, standardization and certification methods, continuous upgradation of course curriculum on Cybercrime , forging of partnership with domestic as well as International Entities etc.

The write up should include complete implementation plan for various Cybercrime Training Modules of NCTC. This entire document should not exceed more than 10 pages.

SL NO.	ACTIVITY	TIMELINE