# Expression of Interest (EOI)

# for

# Central Public Sector Enterprises(CPSEs)

# to

# ESTABLISH CENTERS OF EXCELLENCE (COEs) IN CYBER SECURITY

**All India Council for Technical Education (AICTE)**
**Ministry of Human Resource Development(MHRD)**
**Nelson Mandela Marg, Vasant Kunj**
**New Delhi – 110070**
**Tel Nos.: 011-26131576-78,80**

18th March, 2020

Table of Contents


1. *Letter of Invitation* ..... 3
2. *Background:* ..... 5
3. *Eligibility Criteria* ..... 6
4. *Scope of Work* ..... 7
5. *COE Maintenance* ..... 9
6. *Identification of Industry Partners / Sponsors* ..... 10
7. *Venue & Deadline for submission of proposal* ..... 11
8. *Validity of Offer:* ..... 11
9. *Instructions to CPSE* ..... 12
10. *Evaluation Criteria and Method of Evaluation:* ..... 12
11. *Response:* ..... 12
12. *Commitment to Ethics:* ..... 12
13. *Condition under which EOI is issued:* ..... 12
14. *Last date of submission of EOI:* ..... 13
15. *Formats for Submission:* ..... 13

**Format 1 - Applicant's Expression Of Interest** ..... 13
**Format 2 - Organization Contact Details** ..... 14
**Format 3 – Experience in Related Fields** ..... 15
**Format 4 – List of Experts / Consultants** ..... 16
**Format 5 – Additional Information** ..... 17
**Format 6 – Declaration** ..... 18

## 1. Letter of Invitation

All India Council for Technical Education (AICTE)
Ministry of Human Resource Development(MHRD)
Nelson Mandela Marg, Vasant Kunj,
New Delhi – 110070
Tel Nos.: 011-26131576-78,80

No. AICTE/IDC/COE/2020 Dated:18.03.2020

Dear Sir/Madam,

All India Council for Technical Education (AICTE) under Ministry of Human Resource Development (MHRD) invites sealed Expression of Interest (EOI) from Central Public Sector Enterprises (CPSEs) for establishing Centers of Excellence (COEs) in Cyber Security in identified Educational Institutions across the country under a program involving World Bank funding.

The EOI Document containing the details of qualification criteria, submission requirement, brief objective & scope of work and method of evaluation etc. is enclosed.

You may submit your response in sealed envelopes in prescribed format to the undersigned latest by 01.04.2020.

Institution Development Cell
All India Council for Technical Education(AICTE)
Nelson Mandela Marg, Vasant Kunj
New Delhi – 110070
Tel Nos.: 011-26131576-78,80
Email: advidc@aicte-india.org; ypidc@aicte-india.org

Queries if any may be referred in writing to the Advisor, at the above mentioned address or Telephone No. or at E-mail:

| S.No. | Critical Dates | Date | Time |
|---|---|---|---|
| 1. | EOI issuance Date | 18.03.2020 | 14:00 hrs |
| 2. | EOI Submission Start Date | 18.03.2020 | 14:00 hrs |
| 3. | EOI Submission End Date | 03.04.2020 | 23:59 hrs |

Yours faithfully,

Advisor - II (IDC)
All India Council for Technical Education(AICTE)
Email: advidc@aicte-india.org
Encl.: EOI Document.

## 2. Background:

a) With smart cities emerging rapidly across the globe, there is a massive digital transformation happening within each country and more so in India. There is an urgency to improve protection profile, posture, robustness and resilience of Critical Information Infrastructure (CII) assets against any Cyber-attacks and incidents by both state and non-state actors. For economies across the globe, finding skilled professionals in Cyber Security remains a formidable challenge. Professionals who are not only well-versed with IT fundamentals but also have an aptitude for working in this demanding yet highly rewarding field are required both in quality as well as in substantial numbers.

b) Cyber security risks in smart cities also impacts the global economy at large. The IT sector is one of the major employment generators in any country and a major breach on a smart city could significantly jeopardize future growth within this critical IT sector.

c) The scarcity of cyber security professionals exposes businesses and smart cities to cyber-attacks and reduces their ability to quickly respond to complex threats. In the long run, the cyber risks may discourage companies from implementing new technologies or making new investments in vulnerable smart cities.

d) Demand for security professionals will continue to increase in all sectors due to the unprecedented rise in the number of cyber-attacks. Despite having the largest information technology talent pool in the world, the nation is highly unlikely to produce an adequate number of professionals to close the cyber security skills gap.

e) To address this gap, Centers of Excellence (COE) in Cyber Security must be established to accelerate skill building, capacity building, testing and resilience building for cyber security.

f) NPIU-TEQIP and AICTE have come together to establish at least 10 COE in engineering colleges across the country. The COE shall consist of software and hardware components and the cost of establishment shall be borne equally by TEQIP & Industry/ Sponsors facilitated by implementing CPSE agency / agencies.

g) The COEs will have participation of industry not only in terms of finance but also in enabling institutions to establish vibrant industry-academia linkages. The institute needs to have experienced faculty in the field of Cyber-security

(evident from their credible academic and research experience), and are willing to provide sufficient and distinct space to host the COE along with supporting infrastructure.

h) Establishment of Ten (10) Centres of Excellence (COE) on Cyber Security in TEQIP institutes is under consideration as a part of proposed MoU between AICTE and NPIU (TEQIP).

i) In order to understand the different components and have a feel of such centres, a one-day workshop was organized by AICTE on 28th January 2020 which was attended by 33 nominated TEQIP Institutions.

## 3. Eligibility Criteria

The applicant (CPSE) must quote the Project Management Fee as a percentage of total estimated cost of setting up of each COE in TEQIP institutions to AICTE along with details of tentative Industry sponsors they can facilitate.

| S. No. | Pre-qualification Criteria | Supporting Compliance document |
|---|---|---|
| 1. | The firm must be a Central Public Sector Enterprise (CPSE) | Supporting documents |
| 2. | The firm should be in the business of providing IT/ITES consultancy services for at least 03 years as on31st January 2020 | Certificate by Company Secretary of the applicant's organization |
| 3. | The consultancy firm should at least three cyber security experts as their consultants who is a CISSP or is empaneled under the National Security Database (NSD). | Profile of the consultant. |
| 4. | The firm should not be blacklisted by any Central Govt. / State Govt. / PSU/Govt. Bodies | Declaration signed by the Authorized signatory of CPSE |
| 5. | PAN No. / Service Tax / GST Registration Certificate | Copy of Certificate to be enclosed. |

| | | |
|---|---|---|
| 6. | Preference will be given to agency/organization having prior experience in Review/Appraisal of Centrally Sponsored Scheme for any Central / State Govt. / Govt. Autonomous Bodies. | Provide supporting documents. |
| 7. | The applicant (CPSE) must have office(s) within India. | Address of the office(s) in India. |

AICTE will enter into an MOU with the CPSE for execution of the project, preferably within 7 days of accepting such CPSEs.

## 4. Scope of Work

a) The estimated cost of setting up of each COE in TEQIP institutions would be about INR 2.2 Crores. Out of this INR 2.2 Crores, 50% cost (i.e. INR 1.1 Crore) will be provided by AICTE/NPIU/MHRD and the remaining 50% cost (i.e. INR 1.1 Crore) will be raised by CPSE from the industry partner/sponsor.
b) CPSE is required to function as a system integrator to establish a mix of both physical and virtual technologies to create each COE within 150 days of receiving funds from AICTE.
c) The establishment of all the 10 COEs must not exceed 12 months on the date of receiving funds from AICTE.
d) The CPSE must enter into agreements for a minimum term of 3 years with the respective academic institutions for establishment of COE before commencement of work.
e) The procurement of the technologies must be done in a transparent manner through competent vendors.
f) The COE must incorporate physical and virtual technologies that industry can use for cyber warfare training, simulation and R&D. These advanced IT environments allow companies to practice handling specific real-world scenarios, train employees and customers on the latest threats, and they are essential for combating modern cybercrime. Such environments will also be useful to the military and government agencies, private corporations and entities with a focus on cyber security.
g) **Components of COE**

| S.No. | Component | Features |
|---|---|---|
| 1 | Cyber Physical System | a) Cyber Physical System (CPS) based Smart city simulation with different thematic headings |

| | | |
|---|---|---|
| | Simulation | based on HO Scale models with minimum dimensions of 24 feet x 8 feet<br>b) The platform must have minimum 10 scenarios of cyber security from multiple sectors including Healthcare, Railways / Metro, Water Security, Roads and Transport, Banking and Fintech, Energy Sector etc.<br>c) The CPS simulation model must incorporate PLCs / SCADA devices in the scenarios<br>d) The CPS simulation model must provide hands-on exposure to candidates on IOT and SCADA security and must use Industrial sensors. |
| 2 | Virtual Labs | a) The technology platform must have minimum 150 cyber security scenarios / use cases with vulnerable systems<br>b) The platform must either use virtual machines or containerization technologies.<br>c) The platform must allow access to minimum 20 concurrent sessions<br>d) The platform must provide vulnerable systems as well as attacker consoles with pre-installed tools<br>e) The technology platform must cover scenarios for common cyber security domains such as penetration testing, digital forensics, web application exploitation, Reverse Engineering etc. |
| 3 | Hackathon Platform | a) The hackathon platform must allow creation of standard hackathon contests<br>b) The platform must provide a score-board for the participants / teams<br>c) The platform must provide verification of flags as per contest<br>d) The platform must provide creation of multiple levels of challenges for the contests |
| 4 | SOC Simulation platform | a) The platform must simulate the basic environment of a Security Operations Centre (SOC)<br>b) The platform must utilize open source technologies<br>c) The simulation must enable training of SOC |

| | | |
|---|---|---|
| | | analysts for minimum L1 positions |
| 5 | End Point Detection | a) The end-point-detection must be cross-platform<br>b) The simulation must provide exposure to end-point technologies to the candidates<br>c) The platform must have its own dashboard |
| 6 | Training based on Mitre Attack Framework which is open source | a) Solution must allow testing of attacks based on the open source Mitre Attack framework globally used by the Industry<br>b) The solution must be cross platform. |
| 7 | Threat Intelligence | a) Threat Intelligence feed must be provided to the COE<br>b) The solution must cover minimum<br>(1) blacklisted IPs<br>(2) Malicious Domains<br>(3) Phishing Links<br>c) Threat intelligence must be accessed via an API in most of the industry standard formats like<br>(1) JSON<br>(2) STIX<br>(3) XML<br>(4) CSV<br>(5) Yara Signatures |
| 8 | Cyber warfare scenario Simulation for CXOs / Industry leaders | a) The platform must provide various cyber security scenarios for testing of senior leadership decision making skills<br>b) Must have option to add custom scenarios / Use cases<br>c) Must provide ranking of members for purposes of creation contests and assessments |
| 9 | Digital Forensics Workstation | a) The workstation must provide basic capabilities on Forensic investigations for Mobile devices<br>b) The solution must have tools that provide data recovery and data analysis |

## 5. COE Maintenance

CPSE shall maintain the COE for all hardware and software updates including technical support for 20% of cost of funding received from AICTE for the COE per year for

minimum three years from the date of establishment of COE. The maintenance shall include:

a) Repair or Replacement of any faulty components or electronic parts with manufacturing defect
b) Proper upkeep of the various simulation components
c) Periodic product / software updates including updation of sector-specific threat scenarios, threat intelligence
d) Visit to the COE for routine maintenance twice a year
e) Provide technical support and assistance to the COE for any hardware or software related issues by phone, email or remote support during regular business hours

## 6. Identification of Industry Partners / Sponsors

a) The CPSE must identify suitable industry partners / sponsors who can match the grant provided by AICTE for 10 institutions from the list provided by AICTE for establishment of COE.
b) The CPSE must raise minimum 50% of the cost of COE from the Industry / sponsors.
c) CPSE must provide list of identified industry partners / sponsors while submitting the response to EOI.
d) CPSE must provide list of academic institutions shortlisted by industry partners / sponsors from the list provided by AICTE.
e) To manage the sponsorship terms, CPSE is free to
    a. Identify suitable vendors to manage sponsorship terms of the Industry
    b. Directly enter into separate agreements with host academic institutions in which COE was set up for providing sponsorship benefits to the Industry partner.
    c. Facilitate direct agreements between the Industry sponsor and the academic institution
f) CPSE may directly pick the funding from the Industry if required
g) Industry can also procure any technologies required for COE from the approved components as described in section 4(e)from the sponsorship amount given by them, directly by their choice of vendors if they do not wish to transfer the funds to CPSE.
h) The responsibility of Industry sponsorship is with CPSE and delay of raising funds from the Industry / sponsors by the CPSE must not impact the work and the project must be completed as per given timelines once funds are received by CPSE from AICTE/NPIU/MHRD.

## 7. Venue & Deadline for submission of proposal

Proposal, in its complete form in all respects as specified in the EOI, must be submitted to AICTE at the address specified herein earlier. In exceptional circumstances and at its discretion, AICTE may extend the deadline for submission of proposals, in which case all rights and obligations of AICTE and the applicants previously subject to the original deadline will thereafter be subject to the deadline as extended.

## 8. Validity of Offer:

The offer for EOI as per this document shall be valid for a period of 30 days initially which may be extended further if required by the AICTE.

## 9. Instructions to CPSE

All information as detailed below is to be submitted in two hard copies in separately sealed envelopes and one soft copy by e-wizard portal:

a) Applicant's Expression of Interest as per Format-1.

b) Organizational Contact Details as per Format-2.

c) Experience of the organization as per Format-3.

d) List of three experts/ consultants on payroll as per Format-4.

e) Additional information as per Format-5.

f) Declaration as per Format-6.

g) Power of Attorney in favour of Authorized Signatory with long and short signatures of Authorized person.

h) Consultancy organization must have its office in India.

The applicants are expected to examine all instructions, forms, terms and other details in the EOI document carefully. Failure to furnish complete information as mentioned in the EOI document or submission of a proposal not substantially responsive to the EOI documents in every respect will be at the Applicant's risk and may result in rejection of the proposal.

**10. Evaluation Criteria and Method of Evaluation:**

a) Screening of EOIs shall be carried out as per eligibility conditions mentioned in this document and based on verification of testimonials submitted.
b) EOI will be evaluated for short listing inter alia based on their past experience of handling similar type of project, list of confirmed industry partners / sponsors, strength of their man power, project management fees (as the percentage of estimated cost of setting up of each COE), financial strength of firm and presentation / proposal to the selection committee whose decision will be final.
c) AICTE will take up references and reserves the right to pay due heed to the Applicant's performance elsewhere and any past experience from AICTE.

**11. Response:**

a) Applicants must ensure that their response is submitted as per the formats attached with this document. Special comments on the objectives and scope of the service projected in the enquiry may also be submitted along with the offer.

b) Application in sealed cover super scribed, as "EOI for Engagement of Project Implementing Organization for Establishing Centres of Excellence in Cyber Security for AICTE."

**12. Commitment to Ethics:**

a) The firm shall ensure that vendors shortlisted in procurement are committed for Ethics at workplace.
b) AICTE must be notified immediately by the firm in event any unethical issue or misconduct is identified.

**13. Condition under which EOI is issued:**

The EOI is not an offer and is issued with no commitment. AICTE reserves the right to withdraw EOI and or vary any part thereof at any stage. AICTE further reserves the right to disqualify any applicant, should it be so necessary at any stage.

**14. Last date of submission of EOI:**

The last date of submission of EOI is 01.04.2020 (23:59 hrs.).

**15.Formats for Submission:**

Format 1 - Applicant's Expression of Interest

To,

All India Council for Technical Education(AICTE)

Sub: Submission of Expression of Interest to establish Center(s) of Excellence (COE) in Cyber Security.

Dear

In response to the Invitation for Expression of Interest (EOI) published on 18.03.2020 for the above purpose, we would like to express interest to carry out the above proposed task. The Project Management Fee will be __% of total estimated cost of establishing each COE as described in section 3. As instructed, we attach 2 sets of the following documents in separately sealed envelopes and one softcopy for your kind attention:

1. Organizational Details(Format-2)
2. Experience in related fields(Format-3)
3. List of experts / consultants - at least 3(Format-4)
4. Additional information(Format-5)
5. Declaration(Format-6)

Sincerely Yours,

Signature of the applicant
[Full name of applicant]
Stamp.....
Date:

Encl.: As above.
Note: This is to be furnished on the letter head of the organization.

Format 2 - Organization Contact Details

| S. No | Organizational Contact Details | |
|---|---|---|
| 1. | Name of Organization | |
| 2. | Main areas of business | |
| 3. | Type of Organization Firm/ Company/ partnership firm registered under the Indian Companies Act, 1956/ the Partnership Act, 1932 | |
| 4. | Whether the firm has been blacklisted by any Central Govt. / State Govt./PSU/ Govt. Bodies / Autonomous? If yes, details thereof. | |
| 5. | Address of registered office with telephone no. & fax | |
| 6. | Address of offices in<br>i) National Capital Region of Delhi<br>ii)All other States/UT's | |
| 7. | Contact Person with telephone no. & e-mail ID | |

Enclose: -

1. Copy of Certificate of Incorporation.
2. GST Certificate .

Signature of the applicant
Full name of the applicant
Stamp &Date

Format 3 – Experience in Related Fields

| Experience in Related Fields | | | | | |
|---|---|---|---|---|---|
| Overview of the past experience of the Organization in all aspects related to Brand Building related | | | | | |
| S. No | Items | Number of Assignments during last 5 years | Year the assignment was done | Mention the name of Client/ Organization | |
| 1 | Experience of assignments in IT/ITES sector | | | | |
| 1.1 | Experience in carrying out assignments in Government | | | | |
| 1.2 | Experience in carrying out assignments in Public sector. | | | | |
| | Signature of the applicant<br>Full name of applicant<br>Stamp &Date | | | | |

Format 4 – List of Experts / Consultants

| List of experts/consultants on payroll for Cyber Security (at least 3) | | | | |
|---|---|---|---|---|
| S. No | Name | Designation | Qualification | Weather CISSP or NSD Certified (Yes/No) |
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| 6. | | | | |

Signature of the applicant
Full name of applicant
Stamp & Date

## Format 5 – Additional Information

| Additional Information |
|---|

List of all Industry Partners / Sponsors:

| S.No. | Industry Partner/Sponsor Name |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |

Signature of the applicant
Full name of applicant
Stamp &Date

Format 6 – Declaration

| Declaration: |
| --- |
| We hereby confirm that we are interested in competing for the Project Management work for establishment of COE in cyber security for AICTE.<br><br>All the information provided herewith is genuine and accurate.<br><br>Authorized Person's Signature.<br><br>Name and Designation:<br><br>Date of Signature:<br><br>Note: The declaration is to be furnished on the letter head of the organization. |

*****