Expression of Interest

To

Design, implementation & management Cyber Security initiative of Dr. Babasaheb Ambedkar Technological University, Lonere

INDEX

1 LETTER OF INVITATION

Reference Number:
Date:

Dear Sir/Madam,

Dr. Babasaheb Ambedkar Technological University (DBATU) under State Government of Maharashtra invites Expression of Interest (EOI) for design, implementation and management of Cyber Security Initiative of BATU.

The broad scope will be as follows

1. Design and support of B.Tech Cyber Security course
2. Design and implementation of Centre of Excellence – Cyber Security
3. Purchase and subsequent Maintenance for 5 years of all hardware & Software required for CoE
4. Bringing in Industry partnerships for projects and placements
5. Bringing in National & International Government and University Tie-ups
6. Bringing in expertise from National & International Government Cyber agencies

The entire scope is detailed in this document.

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 prescribed format latest by **dd.mm.yyy (hh:mm hrs)** as a **single Password Protected PDF document**, as an attachment to the Email to be sent to <put email>. The covering email must mention the Name, Email & Mobile Number of the person authorized to disclose the password, when the EOIs are taken up for evaluation by a committee constituted by DBATU. The Email should have "Expression of Interest (EOI) for Design, Implementation & Management of Cyber Security initiative of BATU" mentioned in the Subject line.

Queries if any may be referred in writing to the undersigned.

Yours faithfully,

<Put Name>
<Put Address>
<Put Tel. No,>
<Put Email>

Encl.: EOI Document.

2 BACKGROUND

There is a massive digital transformation happening across the world and along with it came unprecedented increase in Cyber-attacks.

There is an urgency to protect assets against any Cyber- attacks and incidents by both state and non-state actors.

The scarcity of cyber security professionals exposes businesses to cyber-attacks and reduces their ability to quickly respond to complex threats.

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

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.

The COEs will have participation of industry experts to continually grow the expertise. The institute needs to have experienced faculty in the field of Cyber-security and are willing to provide sufficient and distinct space to host the COE along with supporting infrastructure.

To address this gap, DBATU wants to design one of the best Cyber Security Courses along with Centers of Excellence (COE) in Cyber Security to accelerate skill building, capacity building, testing and resilience building for cyber security

3 ELIGIBILITY CRITERIA

This Qualification Criteria is for the main bidder.

The main Bidder can form a consortium of other companies with required experience in the preferences section to deliver the assignment.

#	Pre-qualification Criteria	Supporting Compliance document
1	The firm must be a registered company in India and having offices in India.	Supporting documents
2	The firm should be in the business of providing consulting or services in Cybersecurity for the last 3 financial years. .(FY 20, FY 21, FY 22)	Certificate by Company Secretary of the applicant's organization
3	The firm should not be blacklisted by any Central Govt. / State Govt. / PSU/Govt. Bodies	Declaration signed by the Authorized signatory of CPSE
4	The firm must be a profit-making company for the last 3 Financial years.(FY 20, FY 21, FY 22)	Copy of audited PROFIT AND LOSS STATEMENT .(FY 20, FY 21, FY 22)
5	Last 3 years audited Balance sheet and P&L statement	.(FY 20, FY 21, FY 22)
6	Company must have a positive net worth	Audited net worth of the company AS OF FY 22

4 PREFERENCES

1. Preference will be given to firms/consortium who have prior experience in setting up B.E, B.Tech, Diploma of equivalent courses in Cyber Security
2. Preference will be given to firms/consortium who have set up a CoE in Cyber Security.
3. Preference will be given to Firms/consortium that have track record of Placement.
4. Preference will be given to Firms/consortium that have established relationships with Industries and companies for projects.
5. Preference will be given to the firms/consortium that have established relationships with national and/or international Cyber agencies
6. Preference will be given to the firms/consortium that have established relationships with national & international governments for Cyber security
7. Preference will be given to the firms/consortium that have relationships with International Universities
8. Preference will be given to the firms/consortium who have CISSP certified cyber security experts
9. Preference will be given to the firms/consortium whose individuals are empaneled under the National Security Database (NSD)

5 SCOPE OF WORK

5.1 Design and support of B.Tech Cyber Security Course

The designed course must incorporate all the expertise required to handle all the current trends in Cyber security, both defense and attack. The curriculum of the last semester will be dynamic incorporate the new and emerging trends in Cyber Security so that the students passing out will be up to date in handling all the recent trends. The curriculum of last semester will be designed not more than a year before the beginning of the last semester.

The EoI must also elaborate on your experience of designing and setting this course and how are you proposing to maintain it and keeping it updated for the next 5 years.

The Broad requirement is as below, and you may add to it based on your experience.

1. Design a B.Tech. Cyber Security Curriculum of 4 years (8 semesters)
2. Train the Professors on the above Curriculum
3. Train the Professors every year on the latest trends and ways to handle them.
4. Provide on-line labs from Centre of excellence set-up every semester for students and Professors to practice what they learnt (Both defense and attack)
5. Provide one on-line talk every semester from Cyber Security professionals on current trends.
6. Final year intensive Lab training using Centre of excellence set-up (See below) for hands on training.

5.2 Design and Implementation of Centre of Excellence - Cyber Security

The scope of work is given below for which a budget estimate must be submitted. The purchase and maintenance of the hardware will be the responsibility of the bidder.

The EoI must also elaborate on your experience of setting this up and how are you proposing to maintain it and keeping it updated for the next 5 years.

The Broad requirement is as below, and you may add to it based on your experience.

1. Platform for Physical Cyber Tech Simulation (PPCTS)
    a. The PPCTS 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.
    b. The PPCTS simulation model must incorporate PLCs / SCADA devices in the scenarios
    c. The PPCTS 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 100 cyber security scenarios / use cases with vulnerable systems
    b. The platform must either use virtual machines or containerization technologies.
    c. The platform must allow access to minimum 20 concurrent sessions
    d. The platform must provide vulnerable systems as well as attacker consoles with pre-installed tools
    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. SOC Simulation platform
    a. The platform must simulate the basic environment of a Security Operations Centre (SOC)
    b. The platform must utilize open-source technologies
    c. The simulation must enable training of SOC analysts positions
4. End Point Detection
    a. The end-point-detection must be cross- platform
    b. The simulation must provide exposure to end- point technologies to the candidates
    c. The platform must have its own dashboard
5. 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

b. The solution must be cross platform

6. Threat Intelligence
    a. Threat Intelligence feed must be provided to the COE. The solution must cover minimum
        i. blacklisted IPs
        ii. Malicious Domains
        iii. Phishing Links
    b. Threat intelligence must be accessed via an API in most of the industry standard formats like
        i. JSON
        ii. STIX
        iii. XML
        iv. CSV
        v. Yara Signatures
7. Cyber warfare scenario Simulation for CXOs
    a. The platform must provide various cyber security scenarios for testing of senior leadership decision making skills
    b. Must have option to add custom scenarios / Use cases
    c. Must provide ranking of members for purposes of creation contests and assessments
8. Digital Forensics Workstation
    a. The workstation must provide basic capabilities on Forensic investigations for Mobile devices
    b. The solution must have tools that provide data recovery and data analysis
9. Hackathon Platform
    a. The hackathon platform must allow creation of standard hackathon contests
    b. The platform must provide a scoreboard for the participants / teams
    c. The platform must provide verification of flags as per contest
    d. The platform must provide creation of multiple levels of challenges for the contests

5.3 COE Purchase & Maintenance

The bidding firm shall purchase & maintain the COE for all hardware and software updates including technical support for a period of 5 years. The maintenance shall include:

1. Repair or Replacement of any faulty components or electronic parts with manufacturing defect
2. Proper upkeep of the various simulation components
3. Periodic product / software updates including updation of sector-specific threat scenarios, threat intelligence
4. Visit to the COE for routine maintenance twice a year
5. 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

The estimated yearly budget for maintenance must be indicated.

5.4 Industry Partnerships for Projects and Placements

The bidding firm shall bring top industries

1. To provide projects for students in Cyber Security
2. To engage in Campus recruitment
3. To avail the use of CoE for their employees

The bidder must elaborate their previous experience in this.

5.5 National and/or International Government Partnerships

The bidding firm shall facilitate International Government and International University partnerships with BATU's program.

The bidder must elaborate their previous experience in this.

5.6 International University Partnerships

The bidding firm shall facilitate International University partnerships with BATU's program.

The bidder must elaborate their previous experience in this.

6 Evaluation Criteria and Method of Evaluation and next steps

1. Screening of EOIs shall be carried out as per eligibility conditions mentioned in this document and based on verification of testimonials submitted.
2. EOI will be evaluated for short listing based on the preferences listed.
3. BATU will take up references and reserves the right to pay due heed to the Applicant's performance elsewhere and relevant experience.
4. Shortlisted bidders will be called for a detailed presentation to a specially constituted committee. The presentation will be of 1 hour to present the credentials, experience and methodology of implementation along with budgetary prices. Focus to be given on each item of the scope of work and your capability to implement and execute it.
5. Based on the presentation, the bidders will be finalized.
6. After evaluating the bidders based on their presentation, BATU will formulate a Request for Price (RFP).
7. The finalized bidders shortlisted from the presentation, will be selected for responding to the RFP.

Note: Budgetary cost will be used for initial estimates and will not be considered for evaluation of bidder.

7 Response

1. 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.
2. EOI document has to be submitted as a single Password Protected PDF, as an attachment to the Email to be sent to <put email id> The email must mention the Name, Email & Mobile Number of person authorized to disclose the password, when the EOIs are taken up for evaluation by a committee constituted by BATU. The Email should have "Expression of Interest (EOI) for Design, Implementation & Management of Cyber Security initiative of BATU" mentioned in the Subject line.

8 Condition under which EOI is issued

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

The decision of BATU will be final.

9 APPENDIX

9.1 Applicants Expression of Interest

To,
<BATU to Fill>

Sub: Submission of Expression of Interest (EOI) for Design, Implementation & Management of Cyber Security initiative of BATU.

Sir/Madam,

In response to the Invitation for Expression of Interest (EOI) published on <BATU to Fill> for the above purpose, we would like to express interest to carry out the above proposed task.

We have attached 2 copies of the response to EoI with the following documents in separately sealed envelopes and one softcopy for your kind attention:

1. Company Brief
2. Organizational Details
3. Qualification criteria details
4. Experience in related fields
5. List of Industries with relationships for placement
6. List of experts / consultants - at least 3
7. List of Industry Organizations
8. List of International Organizations affiliated to
9. List of International Universities with relationships
10. Estimated Budgetary Costs
11. Additional information
12. Summary

Authorized Signatory name

Signature with Stamp

Date:

9.2 Company Brief

Company brief in one page

9.3 Organization Details

#	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. & email	
6.	Address of offices in i) Maharashtra 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

9.4 Qualification Criteria Details

Attach all the requested documents listed in qualification criteria.

9.5 Experience in Setting up of course in cyber security

Put N/A if not undertaken

#	Items as per scope defined earlier	Number of assignments undertaken	Year of last assignment	Name of organization where implemented with contact person's name, email and mobile number
1	Design and support of B.E., B.Tech, Diploma or equivalent course on Cyber Security Course			

Signature of the applicant

Full name of applicant

Stamp &Date

9.6 Setting up of CoE for Cyber Security

Put N/A if not undertaken

#	Items as per scope defined earlier	Number of assignments undertaken	Year of last assignment	Name of organization where implemented with contact person's name, email and mobile number
1	Design and Implementation of Centre of Excellence - Cyber Security			
2	COE Purchase & Maintenance			

Signature of the applicant

Full name of applicant

Stamp &Date

9.7 List of Industry Organizations for placements

S. No	University or educational institute name	Number of Students placed	Year of placement	Name of organization with contact person's name, email and mobile number
1.				
2.				
3.				
4.				
5.				
6.				

S. No	Company name	Number of Students placed	Year of placement	Name of organization with contact person's name, email and mobile number
1.				
2.				
3.				
4.				
5.				
6.				

Signature of the applicant

Full name of applicant

Stamp &Date

9.8 List of Industry Organizations for projects

S. No	University or educational institute name	Number of Students projects	Year of project	Name of organization with contact person's name, email and mobile number
1.				
2.				
3.				
4.				
5.				
6.				

S. No	Company name	Number of Students projects	Year of project	Name of organization with contact person's name, email and mobile number
1.				
2.				
3.				
4.				
5.				
6.				

Signature of the applicant

Full name of applicant

Stamp &Date

Please give narration of 10 student projects in not more than 100 words each.

9.9 List of National and International Cyber Organizations affiliated to

S. No	Organization Name	Details of affiliation	Name, email and contact person
1.			
2.			
3.			
4.			
5.			
6.			

Signature of the applicant

Full name of applicant

Stamp &Date

9.10 List of International Government affiliation wrt Cyber security

S. No	Government Name	Details of affiliation	Name, email and contact person
1.			
2.			
3.			
4.			
5.			
6.			

Signature of the applicant

Full name of applicant

Stamp &Date

9.11 List of International Universities with relationships

S. No	University Name	Country	Details of relationship
1.			
2.			
3.			
4.			
5.			
6.			

Signature of the applicant

Full name of applicant

Stamp &Date

9.12 List of CISSP 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.				

Signature of the applicant

Full name of applicant

Stamp &Date

9.13 List of NSD team members

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

Signature of the applicant

Full name of applicant

Stamp &Date

9.14 Estimated Budgetary Costs

#	Items as per scope defined earlier	One-time cost
1	Design and support of B.Tech Cyber Security Course	
2	Design and Implementation of Centre of Excellence - Cyber Security	
3	COE Purchase	
4	Project management and implementation costs	
	Total (A)	

#	Items as per scope defined earlier	Recurring Cost per year
1	Design and support of B.Tech Cyber Security Course	
2	Design and Implementation of Centre of Excellence - Cyber Security: Include any estimated increase in hardware costs.	
3	Hardware Maintenance costs	
5	Any other recurring costs	
	Total (B)	

TCO will be calculated for 5 years.

TCO calculated as (A) + (B) * 5 =

9.15 Any additional Information

Use free flowing format to further your proposal.

9.16 Summary

Please narrate in one page why your company/consortium is best qualified to take up this assignment.