EXPRESSION OF INTEREST (EOI)

FOR

BEML - CYBER SECURITY STRATEGY ROADMAP
FOR NEXT 3 YEARS

INVITATION FOR EXPRESSION OF INTEREST (EOI) FOR

CYBER SECURITY STRATEGY SUPPORT SERVICES

BEML Limited invites 'Expression of Interest (EOI)' from eligible reputed firms for Cyber Security Strategy Support Services.

This EOI is for conducting technical feasibility study only on No Cost No Commitment basis.

Last date for submission of EOI is **18.01.2024**.

Any further Addendum/ Corrigendum/ Extension of dates, Clarifications/ Responses to bidders' queries in respect of the above EoI shall be posted on BEML website (https://www.bemlindia.in) only and no separate notification shall be issued.

1. SCHEDULE DETAILS:

1.1 For better understanding on the EOI scope & existing BEML landscape, you may please take prior appointment to have F2F / VC meeting with our technical team. For taking appointment, mail should be sent to office.dto@bemlltd.in and should have the subject "**Expression of Interest for BEML – Cyber Security Strategy Road map for next 3 years**".

1.2 The response to the EOI should be submitted through email- office.dto@bemlltd.in, super scribing IN THE EMAIL SUBJECT " **EOI for BEML – Cyber Security Strategy Road map for next 3 years.**

1.3 The due date for submission of EOI is **18.01.2024.**

2. INTRODUCTION:

BEML Limited, a Multi-Technology, Multi-Location, Mini Ratna Schedule-A Company under the Ministry of Defence, is a leading public sector undertaking for manufacturing a wide range of Defence & Aerospace, Mining & Construction and Rail & Metro products.

3. PURPOSE:

- This EOI is issued for inviting responses from prospective firms to express their interest in providing Cyber Security Strategy Support Services.
- This EOI is neither an offer letter nor a legal contract, but an invitation for Expression of Interest on No Cost No Commitment Basis.

4. OBJECTIVE:

BEML is looking for an experienced Cyber Security Strategy Support Service Provider to provide robust security strategies, expert guidance, analysis, mitigation, preparing technical tender documents and recommendations to enhance our ***BEML's Cyber Security Strategy Roadmap for next 3 years***.

5. TECHNICAL REQUIREMENT:

The major requirements are as listed below but not limited to:

- Define effective Cybersecurity program for next 3 years – Strategy, Framework, Policy, Process, Standards, Guidelines, Security Architecture, Operating Model and Organization Structure.
- Assessment of current process landscape to identify gaps and vulnerabilities
- Conduct comprehensive cybersecurity assessments, identifying vulnerabilities, risks, and potential points of attack.
- Collaborate with cross-functional teams to develop and implement tailored cybersecurity strategies that align with the organization's goals and objectives.
- Perform in-depth analysis of security architectures, network designs, and applications to ensure they meet security requirements.

- Advise on the selection, deployment, and configuration of security technologies, tools and solutions as per government guidelines.
- Conduct regular penetration testing and vulnerability assessments to proactively identify weaknesses and recommend remediation measures.
- Assist in the development and documentation of incident response plans for various cyber threats and attack scenarios.
- Assist in preparing tender documents inline with the company's requirement and government guidelines.
- Assist in mitigation of remediation for all IT infrastructure (Network Components, End Point Devices, Servers).
- Provide guidance on compliance with industry regulations and standards, ensuring the organization meets necessary security and privacy requirements.
- Design and deliver cybersecurity training programs for employees to raise awareness about security best practices.
- Stay updated on the latest cybersecurity trends, threats, and technologies to provide timely insights and recommendations to the organization.
- Collaborate with third-party vendors and partners to assess their security posture and ensure alignment with our cybersecurity standards.
- Participate in security audits and reviews, both internal and external, to assess the effectiveness of implemented security measures and strictly mitigate the observations.
- Act as a subject matter expert and provide executive-level briefings on the organization's security posture and ongoing initiatives.
- Assist in evaluating and responding to security incidents, guiding the incident response team through containment, analysis, and recovery efforts.
- Develop IT security policy and operational procedures based on information collected.
- Develop a documented action plan containing policies, practices and procedures that mitigate the identified risks.
- Collaboration with our team to assess vulnerabilities, mitigate vulnerabilities and implement effective measures to safeguard our digital assets and network devices.
- Manage and automate Security Operation Center (SOC) effectively with leading SIEM & SOAR tools.

6. PROCESS:

The following process shall be followed:

- Issue of EOI.
- Receipt of EOI from bidders.
- Evaluation of Bidders post fulfilment of the minimum eligibility criteria including presentation of proposed strategy / roadmap.
- Short listing of eligible EOI bidders based on eligibility criteria and presentation.

7. ELIGIBILITY CRITERIA:

Below Sl. No. 1 to 8 are to be fulfilled by the firm for responding to the EOI.

Sl. No.	Criteria Details	Documents required to be submitted – IDEX Participated Firms	Documents required to be submitted – OTHER Firms	Remarks
1	Brief Details about the Firm	Annexure - A to be submitted.	Annexure - A to be submitted.	
2	Experience Criteria Firm must have Experience in application, infrastructure level security operations, deep understanding of current cyber threats, best practices, mitigation and industry standards.	Firm should be a Winner / Runner / Shortlisted of iDEX in "Cyber Security Challenges" Related documents to be submitted.	Firm must have successfully implemented cyber security projects related to services and mitigation support for Network Components, End Point Devices and Servers in any State / Central Govt / PSU Organization or Private Organization	

			with Company Turnover of Rs.1150 Crs and above. Please provide relevant Purchase Order copies.	
3	Firm must have ISO 9001 & 27001 certified.	Not Mandatory	Please provide valid certificate copies.	
4	Firm should have certified CEH / CISA / CISSP domain expertise on cyber security.	Please provide CV and respective certification.	Please provide CV and respective certification.	
5	Financial turnover for last 3 financial years	Not Mandatory	Please provide CA certified document Or Balance Sheet / Profit & Loss Statement.	
6	The vendor should not have been blacklisted by any government/ PSU/Reputed Listed company for corrupt or fraudulent practices or non-delivery, non-performance on the date of EoI Closing date.	Undertaking document as per Annexure-B to be submitted.	Undertaking document as per Annexure-B to be submitted.	

7	The bidder/OEM must possess all valid certificates as mentioned below and should upload copies of the same: • PAN Number • GST Registration details/ Certificate	Please upload copies of registration certificates and copy of PAN card.	Please upload copies of registration certificates and copy of PAN card.	
8	An Undertaking has to be submitted by the bidders stating that they have read, understood and agreeing to all terms and conditions.	Undertaking document as per Annexure-C to be submitted.	Undertaking document as per Annexure-C to be submitted.	

Note:

- IDEX Winner / Runner / Shortlisted participants must ensure to upload relevant IDEX documents. Else, the firms will be considered under the OTHER firm category for evaluation.
- The Bidders must ensure that the documentary proofs to substantiate clauses above are given, without which their EOI will not be considered.
- BEML reserves the right to seek clarifications from the bidder/s for the documents submitted above by the bidder/s at any point of time during the evaluation.

8. PRESENTATION:

- The firms fulfilling the eligibility criteria will be invited to make a presentation to BEML Committee at a date, time and location notified by BEML.
- Firm to present their understanding, proposed Cyber Security strategy roadmap for next 3 years as a part of the presentation keeping in mind of the objective and technical requirements shared in this EOI.

9. FINAL EVALUATION:

- Firms will be shortlisted by the BEML committee members based on demonstration of their capabilities in the presentation for further course of action as per BEML requirement.
- The travel and lodging arrangements and expenses in this regard will have to be borne by the bidder themselves.

10. TERMS & CONDITIONS:

- BEML reserves the right to accept or reject any responses, in whole or inpart, and to enter into discussions with any one or more prospective bidders on no cost no commitment basis.
- Commercials should not be quoted/indicated at any place and in any form in the EOI response. The response of any respondent quoting/indicating commercials, whether directly or indirectly, will be liable to be summarily rejected.

Annexure - A

DETAILS TO BE FILLED/ UPLOADED BY THE PARTICIPATING FIRM

Sl. No.	Description	Details to be filled/uploaded
1	Name of the Firm & Postal address for correspondence (With name of the Contact Person) with telephone number, fax and email id	
2	Bank Details like Bank account numbers & IFSC code with Banker's Name, Address & Contact No.:	Bank account numbers :- IFSC Code: Banker's Name :- Address :- Contact Number :-

I / we hereby certify that all the information given above is factual.

Signature with date of Authorized signatory

Name: _____

Designation: _____

Firm's Seal:_____

Annexure - B

UNDERTAKING

This is to certify that _____ (Name of the Firm) has not been banned / black listed / debarred from Trade by any Central /State Govt. Dept. / Autonomous Institution / PSUs in India at the time of bidding.

I / we hereby certify that all the information given above is factual.

Signature with date of Authorized signatory

Name: _____

Designation: _____

Firm's Seal:_____

Annexure – C

UNDERTAKING

To:

M/s. BEML LTD
Bangalore-27

Dear Sir,

Having examined the EOI, the receipt of which is hereby duly acknowledged, we, the undersigned, hereby confirming that we read, understood and accepting all the terms & conditions available in the EOI.

Signature with date of Authorized signatory

Name: _____

Designation: _____

Firm's Seal:_____