INVITATION FOR "EXPRESSION OF INTEREST" (EOI)

EOI Title	**Cyber Security Awareness and Training**
EOI Reference Number	**EOI-2021-112**
EOI Date	**13 April 2021**

Introduction:

1. The New Development Bank (NDB) is headquartered in Shanghai, China. The Bank was founded in 2014 by the governments of Brazil, Russia, India, China, and South Africa (hereinafter referred to as "BRICS") and launched in 2015 to mobilize resources for infrastructure and sustainable development projects in these countries and other emerging economies.

Commodity/Project Specifications:

2. **NDB** is inviting "Qualified Vendors" (as defined in other conditions) to submit an Expression of Interest for the following Commodity/Project **as per annexure A.**

Instruction for Response:

3. Price quote shall be for the Specifications as exactly mentioned under Commodity/Project Specifications, wherever there is variance in vendor's specifications, that shall be mentioned in the price quote document under the head "Specification Variance."

4. Price quote shall be submitted on the Letter Head of the vendor with Signature of "Authorized person" (as defined in other conditions) and Seal.

5. Price quote shall be submitted only in PDF format.

6. The response shall be only in English language, response in any other language may not be considered.

7. All responses shall have the **EOI title and EOI Number as the subject matter of the mail.** Any mails without title of the EOI will be rejected.

8. Pricing quote shall include tax, installation cost, transportation cost and all other costs if any.

9. Conditions if any to the pricing shall be mentioned in the quote.

10. Any response beyond the submission deadline date shall not be considered unless otherwise submission deadline is extended in writing.

11. The response to this EOI with **EOI Title and EOI Number as the mail subject** should be forwarded to:

    a The technology details, checklist for technology etc. if any to be submitted to botha.dusty@ndb.int

    b Price Quotation to be submitted as password protected files to itsd@ndb.int

    c. Password to be communicated with subject line of the product to baryshnikov.alexander@ndb.int

12. Brief introduction and Credentials of the vendor shall be provided as a separate PDF attachment to Price Quote.

EOI Submission Deadline:

13. The deadline for EOI submission is before **5.00 PM, 26 April 2021**

Other Conditions:

14. Qualified vendors hereby defined as Vendors who are legally in existence with valid business license to operate, who are authorized to deal, sell and or implement on the commodity and or service mentioned in the EOI.

15. Authorized person is hereby defined duly authorized to represent the vendor to provide Technical and commercial quote.

16. The evaluation process and decision taken by NDB will be final. NDB do not have any obligation to disclose the details or results of the evaluation.

17. Responding to this Expression of interest does not constitute any contractual obligation and rights on the part of the vendor.

18. NDB does not responsible for any cost incurred by the vendor towards preparing and submitting the response to the EOI.

19. NDB reserve its rights to cancel the EOI at any stage of the process without assigning any reason and intimation.

20. All the documents including Annexures if any are forming part of the EOI.

Annexure A

General NDB Requirements:

- Program Audience & Scope: Cyber Security Awareness training should be delivered to every member of the NDB. All staff must be included because every individual represents a separate security risk.

- Comprehensive Cyber Security Awareness Training: The cyber security program should include a mix of learning formats and activities,
    - E-Learning
    - Personalized campaigns
    - Videos
    - Guides
    - Instructor-led
    - Feedback Surveys
    - Quizzes
    - Gamifications
    - Phishing, Ransomware attack, Financial Malware attack Exercises
    - Posters
    - Periodic unscheduled awareness assessments to assure compliance with the training.

- The cyber security awareness training needs to be delivered in plain language: Keep things simple and engaging by communicating in plain and common language.

- The cyber security awareness training should be to the point and Fun: Where possible, distill actions into clear cyber security Do's and Don'ts. Provide real-life examples.

- The cyber security awareness training should be measurable:
    - What was the impact of the cyber security awareness training?
    - Are the staff more cyber savvy?
    - Are the staff asking more security related questions?
    - How did the staff find their cyber security training?
    - Are there any aspects of the training that can be improved?
    - Continuous monitoring is important.