Ref.: STPI/BLR/ADM/PERS/TRNG/2022-2023/1 **Date: 21.02.2025**

Annexure – A

- The proposal should be addressed to:

  The Director,
  Software Technology Parks of India.
  Plot No. 76, 77 & 78, 3rd Floor, STPI Building,
  Electronics city, Hosur Main Road,
  Bangalore – 560 100.

- The quote (seal and signed Annexure-A, B, C & D and relevant documents) with **sealed cover** should be addressed to **The Director, STPI-Bengaluru** & should reach this office **ONLY through Post/Courier/by Hand**.

- The quote should reach us **on or before 03.03.2025 at 15:30 Hrs.** The quotation received after the due date will not be accepted.

- The validity of the quote should be 90 days from the last date of submission. The training fee quoted shall be valid for a period of one year.

1. SCOPE OF WORK

- **Course:** Training program on security audit for Mobile Application (Android and iOS) & API Application at STPI-Bengaluru
- Training program on security audit for Mobile Application (Android and iOS) & API Application
- **Training Type:** Physical mode (At STPI Bengaluru office premises)
- **Training Topics:** A detailed outline of the training topics are mentioned in the Annexure-B.
- **No. of Days:** Minimum of 5 days /40 hours of VAPT training for security audit for Mobile Application (Android and iOS) & API Application
- **Batch Size:** Minimum of 12 participants
- **Methodology:** PPT presentations. It should be highly interactive and Hands-on practical session to the participants, case studies, experience sharing with question & answer sessions.
- **Certificate:** Participation Certificate to all participants
- **Trainer Profile:** The trainers shall possess necessary and sufficient domain expertise especially in the security audit of Mobile and API Pentest (i.e.,

Information security Audit) with extensive practical knowledge supported by relevant certifications with minimum of 5 years' experience with relevant area (Android and iOS) & API Application (i.e. Trainers' profiles, experience certificates, certifications, etc.)

- The trainer should set up the required/necessary LAB environment on the cloud or participant laptops and provide a list of tools used in the training program
- **Training Material:** Based on the training topics mentioned in Annexure-B necessary and sufficient course materials shall provide to all participants.
- **Facility:** STPI-Bangalore Auditorium is well equipped with modern facilities to conduct such training.

2. PRICING

- The training cost for security audit for Mobile Application (Android and iOS) & API Application at STPI-Bengaluru for a batch of minimum 12 participants to be provided as per Annexure-D
- Travel, accommodation charges etc. shall be borne by the bidder.
- The price quoted should be exclusive of Tax. Taxes if any should be shown separately.

3. BIDDER ELIGIBILITY CRITERIA

- The bidder must be authorized to provide training in the security audit domain, specifically for Mobile (Android and iOS) and API Applications, with relevant documentation as proof.
- The bidder shall be in the relevant field and should have conducted similar training to any Central/State Govt./PSU/Private companies. The documentary evidence to be provided. (PO/Work orders copies to be furnished)
- The bidder shall have necessary registration certificate for GSTIN and PAN (Copy of the same shall be furnished as proof of the same)
- Profile of trainers to be submitted along with the sufficient domain expertise especially in the security audit of Mobile and API Pentest (i.e., Information security Audit) with extensive practical knowledge supported by relevant certifications with minimum of 5 years' experience with relevant area /trainer certificate to be issued by any global accreditation body.

4. PAYMENT TERMS

- No advance payment will be made. Payment will be released after completion of the training with issuance of valid certificate of participation. The payment shall be released within 30 days from the date of receipt of invoice.

5. TECHO-COMMERCIAL BID FORMAT

- The techno-commercial bid to be submitted strictly as per Annexure D.

6. CLARIFICATION

- To assist in the examination, evaluation and comparison of bids, STPI may, at its discretion ask the bidder for the clarification of its bid. The request for clarification and the response shall be in writing.

- Please feel free to get in touch with us in case of any clarification / information in this regard on 080-66186107 Email: blr.purchase@stpi.in .

7. PLACEMENT OF ORDER

- STPI shall consider placement of order on the bidder whose offer has been found technically and financially acceptable . STPI has full rights to place order on fully or partially.

8. ARBITRATION

- If, a dispute arises out of or in connection with this contract, or in respect of any defined legal relationship associated therewith or derived there from, the parties agree to submit that dispute to arbitration under the ICADR arbitration rule, 1996 and it's all amendments. The venue of the arbitration shall be at New Delhi. The language of the arbitration proceedings shall be in English.

Annexure-B.

- Mobile Application Security (Android & iOS)(VAPT) Training:
  - Mobile Problems and Opportunities
  - Challenges and opportunities for secure mobile phone deployments
  - Weaknesses in mobile devices
  - OWASP Mobile Top 10
  - iOS Architecture
  - Jailbreaking iOS Devices
  - iOS Data Storage and File System Architecture
  - iOS Application Interaction
  - iOS Malware Threats
  - iOS Hands on Labs
  - Android Architecture
  - Rooting Android Devices
  - Android Data Storage and File System Architecture
  - Android Application Interaction
  - Android Malware Threats
  - Android Hands on Labs
  - Android Platform Analysis
- Static Application Analysis
  - Retrieving iOS and Android apps for reverse engineering analysis
  - Decompiling Android applications
  - Circumventing iOS app encryption
  - Header analysis and Objective-C disassembly
  - Swift iOS apps and reverse-engineering tools
  - Android application analysis with MobSF
- Reverse-Engineering Obfuscated Applications
  - Identifying obfuscation techniques
  - Decompiling obfuscated applications
- Dynamic Mobile Application Analysis and Manipulation
- Manipulating and Analyzing iOS Applications
  - Runtime iOS application manipulation with Cycript and Frida
  - iOS method swizzling
  - iOS application vulnerability analysis with Objection
  - Tracing iOS application behavior and API use
  - Extracting secrets with KeychainDumper
  - Method hooking with Frida and Objection
- Manipulating and Analyzing Android Applications
  - Android application manipulation with Apktool
  - Reading and modifying Dalvik bytecode
  - Adding Android application functionality, from Java to Dalvik bytecode
  - Method hooking with Frida and Objection
- Mobile Application Security Verification Standard
  - Step-by-step recommendations for application analysis
  - Taking a methodical approach to application security verification

- Common pitfalls while assessing applications
- Detailed recommendations for jailbreak detection, certificate pinning, and application integrity verification
- Android and iOS critical data storage: Keychain and Keystore recommendations

- Penetration Testing
  - Intercepting TLS Traffic
  - Man-in-the-Middle Troubleshooting
  - Using Mobile Device Remote Access Trojans
- API Security Audit Testing:
  - Introduction to API Security
  - Basics of API fundamental
  - Common vulnerabilities and attack vectors in APIs should cover OWASP Top 10 API Security Risks
  - API authentication, authorization, and data integrity
  - Tools and methodologies for API security testing
  - Assessing the resilience of APIs to various types of attacks
  - Penetration Testing Techniques for APIs
  - Hands-On Practical Labs
  - Real-World Case Studies
  - API Security Tools Overview
  - Securing APIs – Best Practices

Ref.: STPI/BLR/ADM/PERS/TRNG/2022-2023/1 **Date: 21.02.2025**

Annexure- C

	Details
Course Name	Training program on security audit for Mobile Application (Android and iOS) & API Application at STPI-Bengaluru as per the content mentioned in the Annexure-B
Training Type	Physical mode (At STPI Bengaluru office premises)
Training Objectives	State the specific learning objectives and outcomes that the participant would acquire or be able to do after completion of the training
Training Contents	Provide a summary of the proposed training that identifies the essential subject matter contents.
Training Duration:	Specify the duration of training
Batch Size	Provide the maximum no. of participants accommodated in a batch.
Methodology	Provide the course structure giving details of the delivery method to be used in the training. Also, describe all the interactive activities that would be incorporated into the training.
Details of the Certificate	Provide the details of certificate that would be awarded on successful completion of the training.
Trainer Profile	Provide a complete profile of each proposed trainer. (Summary of total experience, relevant experience and certification).
Overview of training material	Provide a brief overview of the material that would be offered. NOTE: Each participant should be provided with course handouts.
Facility Requirements	Mention the facility requirements.

(Authorized Signatory for the Bidder with Seal & Date)

Ref.: STPI/BLR/ADM/PERS/TRNG/2022-2023/1 **Date: 21.02.2025**

Annexure- D

Sl. No.	Item Description	Batch Size	Training Cost (In INR.)
1.	**In-house Training on:** Security audit for Mobile Application (Android and iOS) & API Application at STPI-Bengaluru as per the content mentioned in the Annexure-B		
		Taxes if any	
		Grand Total	

Total in words:

NOTE: Taxes should be indicated as applicable.

(Authorized Signatory for the Bidder with Seal & Date)