

REQUEST FOR PROPOSAL FOR APPOINTMENT OF AUDITOR FOR CONDUCTING INFORMATION SECURITY AND CYBER SECURITY AUDIT

Date: 05-Mar-2024

Corrigendum - 1

| SrNo | Description | Existing Clause | Amended Clause |
|------|--|--|---|
| 1 | Eligibility Criteria Point No.4 Pg. No. 9 in Buyer Specific Added ATC | Criteria -Audit Firm should be based within MMRDA region. Documents to be submitted by Bidder/OEM - Registered office Address Proof (Self certified Copy) | Criteria -Audit Firm should be based within Maharashtra State. Documents to be submitted by Bidder/OEM - Registered office Address Proof (Self certified Copy) |
| 2 | Eligibility Criteria Point No.7 Pg. No. 9 in Buyer Specific Added ATC | Criteria - For SOC 2 Audit: Bidder should be registered with the Institute of Chartered Accountants of India (ICAI) Documents to be submitted by Bidder/OEM - Valid Certificate for ICAI membership | Removed |
| 3 | Eligibility Criteria Point No.8 Pg. No. 10 in Buyer Specific Added ATC | Criteria - The bidder should have on payroll – 1. For IT Audit: at least 5 Auditors who are CISA/CISSP qualified or equivalent; 2. For SOC-2 Audit: at least 5 Auditors having ICAI / AICPA membership; 3.2. For Red Team Assessment: at least 05 Offensive Security Certified Professional (OSCP) from offensive-security / Certified Ethical Hacker (CEH) from EC-Council / Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification; Documents to be submitted by Bidder/OEM -All Relevant certificates/documents supporting basis laid out in pre- qualification criteria. | Criteria - The bidder should have on payroll – 1. For IT Audit: at least 5 Auditors who are CISA/CISSP qualified or equivalent; 2. For Red Team Assessment: at least 05 Offensive Security Certified Professional (OSCP) from offensive-security / Certified Ethical Hacker (CEH) from EC-Council / Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification; Documents to be submitted by Bidder/OEM - All Relevant certificates/documents supporting basis laid out in pre-qualification criteria. |

REQUEST FOR PROPOSAL FOR APPOINTMENT OF AUDITOR FOR CONDUCTING INFORMATION SECURITY AND CYBER SECURITY AUDIT

| | | | |
|---|---|--|--|
| 4 | Eligibility Criteria Point No.10 Pg. No. 10 in Buyer Specific Added ATC | <p>Criteria</p> <p>1. For IT Audit: The proposed Lead Auditor should be Graduate with CISA/CISSP certification with minimum 05 (five) years' experience in IT Audit related activities.</p> <p>2. For SOC 2 Audit: Graduate with ICAI / AICPA membership with minimum 05 (five) years' experience in SOC Audit related activities.</p> <p>3.2. For Red Team Assessment: Relevant certifications with minimum 05 (five) years' experience in assessment related activities.</p> <p>Documents to be submitted by Bidder/OEM - Resume of proposed resource including list of IT /SOC Audit projects/Red Team Assessment handled during last 05 years in India</p> | <p>Criteria</p> <p>1. For IT Audit & SOC-2 Audit: The proposed Lead Auditor should be Graduate with CISA/CISSP certification with minimum 05 (five) years' experience in IT Audit related activities.</p> <p>2. For Red Team Assessment: Relevant certifications with minimum 05 (five) years' experience in assessment related activities.</p> <p>Documents to be submitted by Bidder/OEM - Resume of proposed resource including list of IT projects/Red Team Assessment handled during last 05 years in India</p> |
| 5 | Section 9: Scope of Work Sub-section 9.4: Audit Activities and Frequency Table B: Relevant Circulars for the Audits mentioned in Table A Pg. 14 | Audit # - 7 Annexure Number - Nil | Audit # - 7 Annexure Number - Annexure 18 |
| 6 | Section 9: Scope of Work Sub-section 9.7: Deliverables Pg. 22 | <p>For SOC-2 Audit:</p> <p>a. Annual Audit report starting from February to January current year covering the Data Center and IT Infra and applications. Report must be submitted by March.</p> <p>b. For SOC 2 - Principles covered are Security, Confidentiality and Availability.</p> <p>c. For SOC 3 report is a public version of the SOC 2 report, which means it can be freely distributed to anyone, including the general public.</p> <p>d. Arrange Certified Audit report from certified member of ICAI/CPA.</p> | <p>For SOC-2 Audit:</p> <p>a. Annual Audit report starting from February to January current year covering the Data Center and IT Infra. Report must be submitted by March.</p> <p>b. For SOC 2 - Principles covered are Security, Confidentiality and Availability.</p> <p>c. For SOC 3 report is a public version of the SOC 2 report, which means it can be freely distributed to anyone, including the general public.</p> <p>d. Arrange Certified Audit report duly attested from certified member of ICAI/CPA. Attestation can be outsourced.</p> |

REQUEST FOR PROPOSAL FOR APPOINTMENT OF AUDITOR FOR CONDUCTING INFORMATION SECURITY AND CYBER SECURITY AUDIT

| | | | |
|--|---|--|--|
| 7 | <p>Section 12: Evaluation of Bids Technical Bid Evaluation (Stage 2) Pg. No. 25 Part A: Bidder's Experience & Resource Strength Sl. No. 2</p> | <p>Parameter - The bidder should have on payroll</p> <p>1. For IT Audit : at least 5 Auditors who are CISA/CISSP qualified or equivalent;</p> <p>2. For SOC-2 Audit : at least 5 Auditors having ICAI / AICPA membership;</p> <p>3. For Red Team Assessment : at least 05 Offensive Security Certified Professional (OSCP) from offensive-security / Certified Ethical Hacker (CEH) from EC-Council / Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification;</p> <p>Method of Allocating Marks -</p> <p>a) Minimum 5 in each category = 12 Marks</p> <p>b) More than 5 nos. to 10 nos. in each category = 15 Marks</p> <p>c) More than 10 nos. in each category = 20 Marks</p> <p>Minimum Qualifying Marks - 12</p> <p>Maximum Score - 20</p> <p>Documents Required - Letter from HR along with Resume of resources with valid certifications</p> | <p>Parameter - The bidder should have on payroll</p> <p>1. For IT Audit : at least 5 Auditors who are CISA/CISSP qualified or equivalent;</p> <p>2. For Red Team Assessment : at least 05 Offensive Security Certified Professional (OSCP) from offensive-security / Certified Ethical Hacker (CEH) from EC-Council / Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification;</p> <p>Method of Allocating Marks -</p> <p>a) Minimum 5 in each category = 12 Marks</p> <p>b) More than 5 nos. to 10 nos. in each category = 15 Marks</p> <p>c) More than 10 nos. in each category = 20 Marks</p> <p>Minimum Qualifying Marks - 12</p> <p>Maximum Score - 20</p> <p>Documents Required - Letter from HR along with Resume of resources with valid certifications</p> |
| 8 | Annexure -2 Eligibility Criteria | | Modified |
| 9 | Annexure -18 | | Annexure added for Custody System Audit |
| <p>Note: All other clauses/Terms & conditions except above shall remain same as per RFP (RFP Reference Number: IT-11/2023-24)</p> | | | |