Government of Maharashtra
Office of the Additional Director General of Police,
Maharashtra State Cyber, Home MH Cyber Department, Mumbai, Maharashtra

Request for Proposal for Appointment of Agency for Development, Installation and Maintenance of MahaCyber Safe Mobile Application at Maharashtra Cyber

Bid Document Issued By:

Office of the Additional Director General of Police,
Maharashtra State Cyber,
32nd Floor, Centre - 1, World Trade Centre,
Cuffe Parade, Mumbai - 400005
Tel: 022-22160081
Mobile: +91 8850985498
Email: ig.cbr-mah@gov.in / project.cpaw-mah@gov.in

Contents

Disclaimer

a. Maharashtra Cyber Home MH Cyber Department ("MH Cyber") has taken adequate care in the preparation of the Request for Proposal (RFP Document). Nevertheless, the Bidder should satisfy itself that the RFP Document is complete in all respects. Intimation of any discrepancy shall be given to this office immediately. If no intimation is received by this office, from any Bidder within five days from the date of issue of this document, it shall be considered that the issued document, which has been received by the Bidder, is complete in all respects.

b. Neither MH CYBER, nor its employees, consultants, advisors accept any liability or responsibility for the accuracy or completeness of, nor make any representation or warranty - express or implied, with respect to the information contained in the RFP Document, or on which the RFP Document is based, or any other information or representations supplied or made in connection with the Selection Process.

c. Neither MH CYBER nor its employees or consultants will have any liability to any Bidder or any other person under any law, statute, rules or regulations or otherwise for any loss, expense or damage which may arise from or be incurred or suffered in connection with any information contained in this RFP Document, any matter deemed to form part of this RFP Document, the award of the Project, the information and any other information supplied by or on behalf of MH CYBER or their employees or any consultants or otherwise arising in any way from the Selection Process for the Project.

d. The RFP Document does not address concerns relating to diverse investment objectives, financial situation and particular needs of each party. The RFP Document is not intended to provide the basis for any investment decision, and each Bidder must make its / their own independent assessment in respect of various aspects of the techno-economic feasibilities of the Project. No person has been authorized by MH CYBER to give any information or to make any representation not contained in the RFP Document.

e. Nothing in the RFP Document is, or should be relied on, as a promise or representation as to the future. In furnishing the RFP Document, neither MH CYBER, nor its employees, advisors undertake to provide the recipient with access to any additional information or to update the RFP Document or to correct any perceived inaccuracies therein.

f. MH CYBER or its authorized officers / representatives / advisors reserve the right, without prior notice, to change the procedure for the selection of the Successful Bidder or terminate discussions and the delivery of information at any time before the signing of any agreement for the Project, without assigning reasons thereof.

g. MH CYBER reserves the right to reject any or all the Bids submitted in response to the RFP Document at any stage without assigning any reasons whatsoever. And MH CYBER also reserves the right to change any or all the provisions of the RFP Document. Such changes will be intimated to all the Bidders.

h. Upon the receipt of this RFP Document the Bidder acknowledges the Terms and Conditions of this RFP Document. MH CYBER further reserves the right to change, modify, add to or alter the Selection Process including additional Evaluation Criteria. Any change in the Selection Process shall be intimated to all Bidders.

1. Invitation of Proposal

a) MH Cyber hereby invites Proposals from reputed, competent and professional Information Technology (IT) Services companies, who meet the minimum eligibility criteria as specified in this bidding document for the "***Selection of Service Provider for Development, Implementation and Support of MahaCyber Safe Mobile Application***" as detailed in the RFP document.

b) The complete bidding document shall be published on https://mahatenders.gov.in/ for the purpose of downloading. The downloaded bidding document shall be considered valid for participation in the electronic bidding process (e-Procurement/ e-Tendering) subject to the submission of required tender/ bidding document fee and EMD online, failing which the bid will be summarily rejected.

c) Bidders are advised to study this RFP document carefully before submitting their proposals in response to the RFP Notice. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.

2. Notice Inviting Tender

Sr. No.	Particulars	Details

1.	Name of Work	Appointment of Agency for Development, Implementation and Support of MahaCyber Safe Mobile Application for 5 years.
2.	Earnest Money Deposit (EMD)	INR 5,00,000/- (Five Lakhs) through E-Portal
3.	Tender Publishing Date & Time	12-02-2026; 5:30 PM
4.	Start of Downloading of Tender from E-Tendering Website	12-02-2026; 5:30 PM
5.	Pre-Bid Meeting (Date, Time & Venue)	24-02-2026; 12:30 PM
6.	Last Date & Time for Submission of Tender	09-03-2026; 3:00 PM
7.	Public Opening of Technical Bid	10-03-2026; 3:00 PM
8.	Validity of Tender	180 days from the date of tender opening

The Office of the Additional Director General of Police reserves the absolute right, at its sole discretion, to accept, reject, or modify any or all tenders, without assigning any reason whatsoever. The Authority also reserves the right to award the tender in parts, if deemed necessary to facilitate quicker completion of work, or to withdraw/discharge the tender process at any stage without any prior intimation.

Contact Information:

For any further information or clarification, tenderers may contact:

Office of the Additional Director General of Police
Maharashtra State Cyber, Home MH Cyber Department
32nd Floor, World Trade Centre, Cuffe Parade, Mumbai – 400 005
Phone: 022-22160081
Email: project.cpaw-mah@gov.in

Site Location:

Cyber Headquarters
Maharashtra State Cyber Headquarters,
102 & 103, Sector 2, Millenium Business Park,
Mahape, Navi Mumbai - 400710

Cyber Office
Maharashtra State Cyber,
32nd Floor, World Trade Centre, Centre - 1,
Cuffe Parade, Mumbai - 400005

Contact Persons:
Shri Navnath Devgude, Project Coordinator: +91 8850985498

3. Introduction

Established in 2016, the Maharashtra Cyber MH Cyber Department is at the forefront of combating cybercrime in Maharashtra. As one of India's pioneering dedicated cybersecurity MH Cyber Departments, MahaCyber employs a multi-faceted approach to address the growing menace of cyber threats. Our focus encompasses the detection, prevention, and prosecution of cybercrimes, as well as fostering cybersecurity awareness among Maharashtra's citizens.

Equipped with state-of-the-art infrastructure, including cutting-edge cyber investigation labs, the MH Cyber Department operates through a robust framework comprising a Command & Control

Centre, Security Operation Centre (SOC), Centre of Excellence (CoE), Technology Assisted Investigation (TAI) and Computer Emergency Response Teams (CERT). With over 70 advanced world class tools and a network of around 50 district Cyber Labs across Maharashtra, connected to its HQ in Mahape, Navi Mumbai, we are well-prepared for forensic investigations and real-time cyber threat analysis.

A dedicated portal facilitates citizen's grievance handling and engagement by providing a platform to report cybercrimes, seek assistance and support, receive advisories and stay informed about latest in cybercrime initiatives through our cybersecurity awareness programs. Maharashtra Cyber actively organizes workshops, training sessions, and awareness campaigns to educate individuals, businesses, and government officials about cybersecurity and related issues.

The Technology Assisted Investigation (TAI) function / Forensic lab and Computer Emergency Response Team (CERT) is equipped with world class Cutting Edge Tools & Technologies.

Our vision is to foster a digitally resilient and secure society, where individuals and organizations can utilize digital public goods and amenities, provided by government as well academia, industry in engaging with technology safely, confidently to safeguard themselves from cyber fraudsters. We aspire to create a future where cybersecurity is a collective responsibility, while everyone is enabled with knowledge and tools needed to safeguard themselves from online threats. Our goal is to cultivate a culture of cybersecurity awareness and preparedness that encourages innovation, public participation, trust, and confidence in the digital world.

The MahaCyber Security Project is designed with a fivefold objective for the state of Maharashtra:

1. Providing Accessible Channels: Offering user-friendly avenues for citizens to report Cybercrimes.
2. Protecting Infrastructure: Safeguarding Critical National and Information Infrastructure from malicious activities.
3. Enhancing Investigation Efficiency: Streamlining cybercrime investigations by leveraging integrated digital tools and establishing new Standard Operating Procedures (SOPs).
4. Empowering Investigators: Equipping Investigating Officers (IOs) with the necessary technology tools, training, and operational expertise.
5. Raising Awareness: Increasing public awareness about cybercrimes and digital fraud.

4. Project Background

The MahaCyber Safe Mobile Application is envisaged as a comprehensive, citizen-centric cybersecurity platform designed to assist residents of Maharashtra in identifying, understanding, and responding to cyber-related risks and threats. The application is intended to function as an always-available digital safety companion, providing real-time guidance, awareness, and protective insights to citizens through an intuitive mobile interface.

The application shall deliver mobile-based cybersecurity awareness and protection services through features such as real-time scanning, security alerts, threat identification, and proactive risk mitigation. By integrating multiple cybersecurity modules, including QR code and URL scanning, Wi-Fi security assessment, OTP security checks, data breach verification, application permission analysis, and device-level security advisory mechanisms, the platform shall enable users to assess potential cyber risks and take informed actions to safeguard their mobile devices and online identities.

The MahaCyber Safe Mobile Application shall be supported by a centralized administrative system that enables authorized personnel to manage configurations, update cyber awareness content, monitor application usage, and review analytical insights. The system shall also facilitate oversight by designated government authorities through access to system-level reports and dashboards, supporting informed decision-making and policy formulation.

Overall, the MahaCyber Safe Mobile Application aims to strengthen Maharashtra's cyber safety ecosystem by improving citizen awareness, enabling timely identification of cyber threats, reducing exposure to digital fraud, and establishing a scalable, technology-driven framework for cybersecurity awareness, monitoring, and governance.

5. Instructions to bidders

The Office of ADG-Cyber, Government of Maharashtra will select companies competing as a single entity in accordance with the method of selection specified in these 'Instructions to Bidders' (ITB) for **Selection of Service Provider Development, Implementation and Support of MahaCyber Safe Mobile Application for 5 years**. This Request for proposal is open to all Bidders meeting the pre-qualification criteria of the RFP.

5.1. General

a) While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements. Bidders and recipients of this RFP may wish to consult their own legal advisors in relation to this RFP.
b) All information supplied by Bidders shall be treated as contractually binding on the Bidders, on successful award of the assignment by Office of ADG-Cyber, Government of Maharashtra based on this RFP.
c) No commitment of any kind, contractual or otherwise, shall exist unless and until a formal written contract has been executed by or on behalf of Office of ADG-Cyber, Government of Maharashtra. Any notification of preferred bidder status by Office of ADG-Cyber, Government of Maharashtra shall not give rise to any enforceable rights by the Bidder. Office of ADG-Cyber, Government of Maharashtra may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of Office of ADG-Cyber, Government of Maharashtra.

d) This RFP supersedes and replaces any previous public documentation & communications and Bidders should place no reliance on such communications.

5.2. Purpose

The purpose of this RFP is to seek the services of reputed firm/agency, which shall Development, Implementation and Support of MahaCyber Safe Mobile Application for 5 years. This document provides information to enable the bidders to understand the broad requirements to submit their bids.

5.3. Transfer of RFP

The RFP Document is not transferable to any other bidder. Bidder who purchases the document and submits the Bid shall be the same.

5.4. Eligibility

The eligibility of the Bidder will be adjudged based on the prequalification criteria mentioned in the RFP document. The Financial and Technical credential of the Single Entity shall only be considered for evaluating the proposal. The Bidder should meet the requirement of submission of EMD.

5.5. Examination of RFP

In preparing the Proposal, Bidder is expected to examine in detail the documents comprising the RFP. Material deficiencies in providing the information requested in the RFP documents may result in rejection of a Proposal.

5.6. Conflict of Interest

MH Cyber Department requires that Bidder provides professional, objective and impartial advice and always holds the MH Cyber Department interest's paramount, avoids conflicts with other assignments or their own corporate interests and act without any consideration for future work. Bidder shall not be recruited for any assignment that would conflict with their prior or current obligations to other clients, or that may place them in a position of not being able to carry out the assignment in the best interest of the MH Cyber Department.

5.7. Compliant Proposals / Completeness of Response

a) Bidder is advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.
b) Failure to comply with the requirements of this paragraph may render the Proposal non-compliant and non-responsive and the Proposal may be rejected. Bidders must:
    I. Include all documentation specified in this RFP.
    II. Follow the format of this RFP and respond to each element in the order as set out in this RFP.

5.8. Fraud and Corruption

a) The Bidders is required to observe the highest standard of ethics during the procurement and execution of such contracts. In pursuance of this policy, the following shall apply:

For this provision, the terms are defined and are set forth as follows:

i. **"Corrupt Practice"** means behaviour on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves and/or those close to them, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution.

ii. **"Fraudulent Practice"** means a misrepresentation of facts to influence a procurement process or the execution of a contract to the detriment of the borrower and includes collusive practices among bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the borrower of the benefits of free and open competition.

b) MH Cyber Department will reject Proposal for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract.

c) MH Cyber Department will declare a Bidder ineligible either indefinitely or for a stated period, to be awarded a contract if it, at any time, determines that the Company has engaged in corrupt or fraudulent practices in competing for, or in executing, and the assignments awarded by MH Cyber Department.

5.9. Participation of Government Employees

a) Government employees are not permitted to undertake any assignment without the approval of the Government as per extant Government rules. In addition, no staff/ relatives of MH Cyber Department staff should be proposed for participation in the assignment.

b) In case the Bidder proposes any Government employee as an Expert, the Bidder shall deploy such personnel within the agreed deployment period and submit the NOC/ approval of the concerned Government MH Cyber Department prior to deployment.

5.10. Consortium

Consortiums of companies is allowed for maximum up to two partners i.e. (Lead bidder and consortium partner).

5.11. Prequalification Criteria

The minimum eligibility criteria that should be satisfied by the Bidders are mentioned below. The formats for the Pre-qualification documents are given in the RFP document, unless specified otherwise.

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
PQ-1	EMD	The Bidder (a) Should have made a payment of ₹ **5,000/-** (INR Five Thousand seven Hundred only including 18% GST) (Non-Refundable) for the Tender Fees. (b) Should have submitted EMD of ₹ 5,00,000/- (INR Five lakhs only) or through Bank Guarantee. **Note:** Any request or waiver for EMD exemption will not be entertained.	• Cost of tender document must be submitted through e-payment only. • EMD to be paid via online Payment Gateway mode. The information of E-Payment Gateway available on E-Tendering Website https://mahatenders.gov.in
PQ-2	Legal Entity	The Bidder or consortium partner	The bidder shall submit following documents:

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
		• Shall be a public listed company. • Shall be registered with GST Authorities in India • Should have their registered offices with legal presence in India	• Copy of Certificate of Incorporation. • Copy of PAN Card • Copy of GST certificate
PQ-3	Turnover	The Bidder or consortium partner should have an average annual turnover of minimum INR 7.5 crore revenue for the last three financial years (FY 2022-23, 2023-24 and 2024-25) from IT/ITES.	The bidder shall submit following documents: • Audited Balance Sheet and Profit & Loss Account Statements of the Bidder for each of the last 3 audited financial years (FY 2022-23, 2023-24 and 2024-25). • Certificate from the statutory auditor/ CA clearly specifying turnover details of the company for financial years (FY 2022-23, 2023-24 and 2024-25).
PQ-4	Financial Strength	The bidder and consortium partner should have positive net worth for the last 3 financial years	The bidder shall submit following document: • Certificate from the Statutory auditor/ Chartered Accountant on the Net Worth / net profit of the company for financial years.
PQ-5	Relevant Experience	The Bidder or consortium partner should have been successfully executed similar project or any Cyber security related project in the last 5 years with Central/ State Government Departments / PSU	The bidder shall submit following documents: • Copy of work order/ Contract clearly highlighting the scope of work and value of the contract / order.
PQ-6	Relevant Experience	The Bidder or consortium partner should have been successfully executed similar projects or any Cyber security related project pertaining. 1) One project with work order value at least 2 Cr. 2) Two projects with each work order value of at least 1.5 Cr. 3) Three projects with each work order value of at least 1 Cr.	• Copy of Work order or completion certificate
PQ-7	Certificate	The Bidder or consortium partner should possess a valid certification for the following, as on the date of submission of bid- • ISO 9001: 2015 • ISO 27001:2022 • CMM level 3	The bidder shall submit copies of valid certificates in the name of the bidding entity.

#	Basic Requirement	Criterion	Supporting documents to be submitted with the Bid
PQ-8	Relevant Experience	The Bidder or consortium partner should have at least 10 technical resources on its payroll as on date of submission of bid.	The bidder shall submit following documents: • Declaration letter from HR on company letter head stating the same.
PQ-9	Blacklisting	The Bidder should not be debarred/ blacklisted by any Government / PSU / Semi- Government Sector in India as on date of submission of the Bid.	Affidavit that the bidder has not been debarred/ blacklisted by any Government / PSU / Semi- Government Sector in India

5.12. Technical Evaluation Criteria

<table>
<tr><th>#</th><th>Criteria</th><th>Evaluation parameters</th><th>Maximum Marks</th><th>Documents Required</th></tr>
<tr><td colspan="5">I. Financial & Professional strength of Bidder – Maximum 20 Marks</td></tr>
<tr><td>TQ 1</td><td>Bidder or consortium partner should have average minimum annual turnover of at least INR 7.5 Crores in the last 3 financial years.</td><td><table><tr><th>Turnover in INR</th><th>Marks</th></tr><tr><td>> 7.5 Crores <=10 Crores</td><td>16</td></tr><tr><td>>10 Cr & <=13 Cr</td><td>18</td></tr><tr><td>> 13 Cr</td><td>20</td></tr></table></td><td></td><td>The bidder shall submit following documents:
• Audited Balance Sheet and Profit & Loss Account Statements of the Bidder for each of the last 3 audited financial years.
• Certificate from the statutory auditor/ CA clearly specifying turnover details of the company.</td></tr>
<tr><td colspan="5">II. Experience – Maximum 30 Marks</td></tr>
<tr><td>TQ 2</td><td>Experience of successfully executing at least two similar projects or any Cyber security related project of minimum value of Rs 1 Cr in last five years</td><td><table><tr><th>Value</th><th>Marks</th></tr><tr><td>> =INR 1 crores & < INR 2 crores</td><td>7</td></tr><tr><td>> =INR 2 crores & above</td><td>10</td></tr></table></td><td></td><td>The bidder shall submit following documents:
• Copy of Work order/ Contract clearly highlighting the scope of work and value of the contract / order
• Copy of Completion Certificate/ Milestone / Phase Completion Certificate issued & signed by the competent authority.</td></tr>
<tr><td>TQ 3</td><td>Experience of number of projects pertaining to development, customization, installation and maintenance of similar mobile application or any Cyber security related project in last five years.</td><td><table><tr><th>Value</th><th>Marks</th></tr><tr><td>> =1 to < 3</td><td>10</td></tr><tr><td>> =3 to <5</td><td>15</td></tr><tr><td>>5</td><td>20</td></tr></table></td><td></td><td>• Copy of Work order/ Contract clearly highlighting the scope of work and value of the contract / order
• Copy of Completion Certificate/ Milestone / Phase Completion Certificate issued & signed by the competent authority.</td></tr>
<tr><td colspan="5">III. Manpower – Maximum 20 Marks</td></tr>
</table>

<table>
<tr><th>#</th><th>Criteria</th><th>Evaluation parameters</th><th>Maximum Marks</th><th>Documents Required</th></tr>
<tr><td>TQ 4</td><td>The Bidder shall have a minimum of 10 IT/ITeS skilled employees. The marks for the same shall be as follows-</td><td><table><tr><th>No. of employees</th><th>Marks</th></tr><tr><td>>= 10 employees & <15 employees</td><td>14</td></tr><tr><td>>= 15 employees & <20 employees</td><td>17</td></tr><tr><td>>20 employees</td><td>20</td></tr></table></td><td></td><td></td></tr>
<tr><td>IV.</td><td colspan="4">Technical Presentation – Maximum 30 Marks</td></tr>
<tr><td>TQ 5</td><td>Technical Presentation must cover the Overall
Overall solution design, architecture, development, security, integration aspects, scalability, workflow and interface with optimum hardware requirement to meet the application SLA.
Approach and methodology to perform the work in this assignment, development plan and implementation plan, operations, management and handholding plan.
Solution readiness for deployment as per functionalities required.</td><td>Technical Presentation:</td><td>NA</td><td></td></tr>
<tr><td></td><td>Grand Total</td><td>100</td><td></td><td></td></tr>
</table>

5.13. Queries / Clarifications on the RFP

Queries / Request for clarifications on the RFP shall be sent by Bidders through email only in the format specified in the RFP not later than the date and time specified in the 'Bidding Schedule'. All the requests shall be addressed to MH Cyber Department contact person assigned as mentioned in the 'Bidding Schedule'. No request for clarification from any Bidder shall be entertained after the last date and time mentioned in the 'Bidding Schedule'.

MH Cyber Department will endeavour to provide a complete, accurate, and timely response to all queries / clarifications to all the Bidders. However, MH Cyber Department shall not make any warranty as to the accuracy and completeness of responses. The response to the queries will be published on https://mahatenders.gov.in/.

5.14. Supplementary Information/Corrigendum/Amendment to the RFP

a) At any time prior to the deadline (or as extended by MH Cyber Department) for submission of bids, MH Cyber Department for any reason, whether at its own initiative or in response to clarifications requested by the Bidder may modify the RFP document by issuing Amendment(s) or issue additional data to clarify an interpretation of the provisions of this RFP. Supplements / Corrigendum to the RFP issued by MH Cyber Department would be displayed on the e-Tendering Portal / Website of MH Cyber Department and may additionally also be communicated by e-mail to the Bidders. Any such Supplement / Corrigendum / Amendment shall be deemed to be incorporated by this reference into this RFP.

b) Any such Supplement / Corrigendum / Amendment will be binding on all the Bidders. MH Cyber Department will not be responsible for any misinterpretation of the provisions of this Tender document on account of the Bidders failure to update the Bid documents based on changes announced through the website.

c) In order to allow Bidders a reasonable time to take the Supplement / Corrigendum / Amendment(s) into account in preparing their bids, MH Cyber Department, at its discretion, may extend the deadline for the submission of bids.

5.15. Proposal Preparation Costs

The Bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of Proposal, in providing any additional information required by MH Cyber Department to facilitate the evaluation process, and in negotiating a definitive Service Agreement and all such activities related to the Bid process. This RFP does not commit MH Cyber Department to Award a Contract.

No reimbursable cost may be incurred in anticipation of award of the Contract for implementation of the Project.

All materials submitted by the Bidder shall be the absolute property of MH Cyber Department and no Copyright /Patent etc. shall be entertained by MH Cyber Department.

5.16. Only One Proposal

If a Bidder submits or participates in more than one Proposal, such a Bidder shall be disqualified.

5.17. Department right to terminate the process

MH Cyber Department makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. Further, this RFP does not constitute an offer by MH Cyber Department. The RFP does not commit MH Cyber Department to enter into a binding Agreement in respect of the Project with the Bidders.

5.18. Modification, Substitution or Withdrawal of Proposals

No Proposal may be withdrawn in the interval between the deadline for submission of Proposals and the expiration of the validity period specified by the MH Cyber Department. Entire EMD may be forfeited if any of the Bidders withdraw their Bid during the validity period.

5.19. Language of Bids

This bid should be submitted in English language only. If any supporting documents submitted are in any language other than English, then the translation of the same in English language is to be duly certified by the Bidder and submitted with the bid, and English translation shall be validated at MH Cyber Department discretion.

5.20. Ownership of Solution and Documents Prepared by the Successful Bidder

All plans, specifications, designs, reports, other documents, patents and software including the source code shall be absolute property of MH Cyber Department. The Successful Bidder shall transfer to MH Cyber Department all Intellectual Property Rights in the Software developed if any. The Successful Bidder shall not use anywhere, without getting permission, in writing, from MH Cyber Department and the MH Cyber Department reserves right to grant or deny any such request.

5.21. Instructions for Online Bid Submission

Proposals must be direct, concise, and complete and must be submitted online only. MH Cyber Department will evaluate the Bidder's Proposal based on its clarity, relevance and the directness of its response to the requirements of the Project as outlined in this RFP.

Bidders shall furnish the required information on their Technical and Commercial Proposals in the enclosed formats only. In case of any deviations in the format Bid will be liable for rejection.

5.22. Procedure for Submission of Bids

- To view Tender Notice, Detailed Time Schedule, Tender Document for this Tender and subsequently download the Tender Document and its supporting documents, kindly visit following e-Tendering website: https://mahatenders.gov.in/.
- The Bidders participating for the first time for e-Tenders on e-tendering portal will have to complete the Online Registration Process for the e-Tendering portal.
- All Bidders interested in participating in the on-line e-Tendering process are required to obtain Class II or Class III Digital Certificates. The tender should be prepared & submitted online using individual's digital signature certificate.

5.23. Commercial Proposal

- Bidders should necessarily give the financial details in the format given in the RFP document. All the financial details should be given in the prescribed format only and in accordance with the details and terms and conditions as mentioned in the RFP. The Bidder is expected to understand the RFP in all respects. In case the Service Provider does not quote for or provision for any hardware / software / any other expenses required to meet the requirements of the RFP, he shall be solely responsible for those and would be required to provide them, without any additional cost to MH Cyber Department.
- The Bidder is expected to price all the items and services proposed in the Technical Proposal. The Bid should be comprehensive and inclusive for all the services to be provided by the Bidder as per the scope of his work and must cover the entire Contract Period.

- MH Cyber Department may seek clarifications from the Bidder on the Technical Proposal. Any of the clarifications by the Bidder on the Technical Proposal should not have any commercial implications. The Commercial Proposal submitted by the Bidder should be inclusive of all the items in the Technical Proposal and should incorporate all the clarifications provided by the Bidder on the Technical Proposal during the evaluation of the technical offer.
- Commercial Proposal shall not contain any technical information.

5.24. Period of Validity of Proposal

- The Proposals shall be valid for 120 days from the Bid Submission End Date. A Proposal valid for a shorter period may be rejected as non-responsive. On completion of the validity period, unless the Bidder withdraws his Proposal in writing, it will be deemed to be valid until such time that the Bidder formally (in writing) withdraws his Proposal.
- In exceptional circumstances, at its discretion, MH Cyber Department may solicit the Bidder's consent for an extension of the validity period. The request and the responses thereto shall be made in writing or by email.

5.25. Correction of Errors in Commercial Proposal

- Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted figures will be entertained after the Commercial Proposals are received by MH Cyber Department.
- The quoted price shall be corrected for arithmetical errors.
- In cases of discrepancy between the prices quoted in words and in figures, lower of the two shall be considered. The successful Bidder is required to execute a contract agreement in the proforma attached with the Bid documents on stamp paper of appropriate value as per Maharashtra Stamp Act, 1958 (as amended from time to time). The contract agreement should be executed within 30 days from the date of receipt of acceptance letter.
- The amount stated in the Commercial Proposal, adjusted in accordance with the above procedure and shall be considered as binding on the Bidder for evaluation.

5.26. Prices and Price Information

- The Bidder shall quote a price for all the components of the solution that are necessary to meet the requirements of the RFP.
- All the prices will be in Indian Rupees.
- All prices should be rounded off to the nearest Indian Rupees (If the first decimal value is 5 (five) or above it should be rounded up and below 5 (five) should be rounded down.
- The price quoted in the Commercial Proposal shall be the only and maximum payment payable by MH Cyber Department to the successful Bidder for completion of the contractual obligations

by the successful Bidder under the Contract, subject to the terms of payment and performance levels specified in this RFP.

- The Total Contract Value should be inclusive of all costs including the costs towards packing, forwarding, transportation, insurance for the Contract Period, delivery charges, travel / stay, daily allowance or any other allowances with respect to their staff deployed for the execution of this Project before or after the award of the Contract.
- The price would be inclusive of all taxes, duties, charges and levies as applicable but excluding GST.
- The prices, once offered, must remain fixed and must not be subject to escalation for any reason whatsoever within the period of the validity of the Proposal and the Contract. No revision of the Total Contract Value shall be made on account of any variations in costs of labour and materials, currency exchange fluctuations with international currency or any other cost component affecting the total cost in fulfilling the obligations under the Contract. A Proposal submitted with an adjustable price quotation or conditional Proposal may be rejected as non-responsive.
- Bidder should provide all prices and quantities as per the prescribed format given in the Commercial Bid format in the RFP document. In case the field is not applicable, Bidder must indicate "0" (zero) in all such fields. In case the Bidder leaves a cell blank, it will be taken as "0" (zero).
- The payments would be made to Agency based on the Total Contract value (inclusive of all taxes, levies, charges and duties but excluding GST) in the Commercial Proposal submitted only, subject to the terms of payment and performance levels specified in the Contract. No additional or separate payment shall be made for services that are to be delivered by the Bidder as part of his scope of work for this Project.
- All costs incurred due to delay of any sort attributable to the Bidder shall be borne by the Bidder.

5.27. Discount

The Bidders are advised not to offer any separate discount. Discount, if any, should be merged with the quoted prices. Discounts of any type, indicated separately, will not be considered for evaluation purposes.

5.28. Conditions under which this RFP is issued

- This RFP is not an offer and is issued with no commitment. MH Cyber Department reserves the right to withdraw the RFP and change or vary any part thereof at any stage. MH Cyber Department also reserves the right to disqualify any Bidder should it be so necessary at any stage.
- Timing and sequence of events resulting from this RFP shall ultimately be determined by MH Cyber Department.

- No oral conversations or agreements with any official, agent, or employee of MH Cyber Department shall affect or modify any terms of this RFP, and any alleged verbal Agreement or arrangement made by a Bidder with any MH Cyber Department, agency, official or employee of MH Cyber Department shall be superseded by the definitive Agreement that results from this RFP process. Verbal communications by MH Cyber Department to Bidders shall not be considered binding on it, nor shall any written materials provide by any person other than MH Cyber Department.
- Neither the Bidder nor any of the Bidder's representatives shall have any claims whatsoever against MH Cyber Department or any of their respective officials, agents, or employees arising out of or relating to this RFP or these procedures (other than those arising under a definitive service Agreement with the Bidder in accordance with the terms thereof).
- Until the Contract is awarded and during the currency of the Contract, Bidders shall not, directly or indirectly, solicit any employee of MH Cyber Department to leave MH Cyber Department or any other officials involved in this RFP process to accept employment with the Bidder, or any person acting in concert with the Bidder, without prior written approval of MH Cyber Department.

5.29. Rights to the Content of the Proposal

All Proposals and accompanying documentation of the Technical Proposal will become the property of MH Cyber Department.

5.30. Non-conforming Proposals

A Proposal may be construed as a non-conforming Proposal and ineligible for consideration:

- If it does not comply with the requirements of this RFP.
- If the Proposal does not follow the formats requested in this RFP or does not appear to address the requirements of MH Cyber Department.

5.31. Disqualification

The Proposal is liable to be disqualified in the following cases or in case the Bidder fails to meet the bidding requirements as indicated in this RFP:

- Proposal not submitted in accordance with the procedure and formats prescribed in this document or treated as non-conforming Proposal.
- During validity of the Proposal, or its extended period, if any, the Bidder increases his quoted prices.
- The Bidder qualifies the Proposal with his own conditions.
- Proposal is received in incomplete form.
- Proposal is not accompanied by all the requisite documents.
- Proposal is not accompanied by the EMD.

- If the Bidder provides quotation only for a part of the Project.
- Information submitted in Technical Proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the Contract (no matter at what stage) or during the tenure of the Contract including the extension period, if any.
- Commercial Proposal if enclosed with the Technical Proposal.
- Bidder tries to influence the Proposal evaluation process by unlawful / corrupt / fraudulent means at any point of time during the Bid process.
- In case any one Bidder submits multiple Proposals or if common interests are found in two or more Bidders, the Bidders are likely to be disqualified, unless additional Proposals/Bidders are withdrawn upon notice immediately.
- While evaluating the Proposals, if it comes to MH Cyber Department knowledge expressly or implied, that some Bidders may have colluded in any manner whatsoever or otherwise joined to form an alliance resulting in delaying the processing of Proposal then the Bidders so involved are liable to be disqualified for this Contract as well as for a further period of three years from participation in any of the RFPs floated by MH Cyber Department.
- If the EMD, Pre-qualification Proposal, Technical Proposal contain any information on price, pricing policy, pricing mechanism or any information indicative of the commercial aspects of the Bid.
- Bidder fails to deposit the Performance Bank Guarantee (PBG) within 15 days or fails to enter a Contract within 30 Business Days of the date of issue of Letter of Acceptance or within such extended period, as may be specified by MH Cyber Department.

5.32. Acknowledgement of Understanding of Terms

By submitting a Proposal, each Bidder shall be deemed to acknowledge that all sections of this RFP, including all forms, schedules, annexure, corrigendum and addendums (if any) hereto, has been carefully read and has been fully informed as to all existing conditions and limitations.

5.33. Bid Opening and Proposal Evaluation Process

5.33.1. Bid Opening Sessions

- Bid opening will be conducted in two stages.
- The Bid submitted without EMD, will be summarily rejected. Only those Bid for which EMD is received will be eligible for opening.
- Total transparency will be observed and ensured while opening the Proposals/Bids.
- MH Cyber Department always reserves the right to postpone or cancel a scheduled Bid opening.
- In the first stage, Pre-qualification Proposals would be opened. The EMD of the Bidders will be opened on the same day and time on which the Pre-qualification Proposal is opened, and

bids not accompanied with the requisite EMD or whose EMD is not in order shall be rejected. Technical Proposals of Bidders who pass the Pre-qualification criteria will be opened.

- In the second stage, Commercial Proposal of those Bidders whose Technical Proposals qualify, would be opened. All Bids would be opened in the presence of Bidders' representatives who choose to attend the Bid opening sessions on the specified date, time and address.
- The Bidders' representatives who are present shall sign a register evidencing their attendance. In the event of the specified date of Bid opening being declared a holiday for MH Cyber Department, the bids shall be opened at the same time and location on the next working day. In addition to that, if their representative of the Bidder remains absent, MH Cyber Department will continue process and open the bids of all bidders.
- During Bid opening, preliminary scrutiny of the Bid documents will be made to determine whether they are complete, whether required EMD has been furnished, whether the Documents have been properly signed, and whether the bids are generally in order. Bids not conforming to such preliminary requirements will be prima facie rejected. MH Cyber Department has the right to reject the bid after due diligence is done.

5.33.2. Overall Evaluation Process

a) The Tender Evaluation Committee constituted by the MH Cyber Department shall evaluate the bids

b) The Tender Evaluation Committee will review the Pre-qualification Proposal of the Bidders to determine whether the requirements as mentioned in the RFP are met. Incomplete or partial Proposals are liable for disqualification. All those Bidders whose Pre-qualification Proposal meets the requirements would be selected for opening of the Technical Proposal.

c) The Tender Evaluation Committee shall review the Technical Proposal of the pre- qualified Bidders to determine whether the Technical Proposals are substantially responsive. Bids that are not substantially responsive shall be disqualified and the Tender Evaluation Committee reserves the right to seek clarification if required.

d) The Tender Evaluation Committee shall assign a technical score to the Bidders based on the technical evaluation criteria detailed in the RFP. The Bidder with a technical score above the threshold as specified in the RFP shall technically qualify for the commercial evaluation stage.

5.33.3. Evaluation of Pre-qualification Proposals

a) Bidders whose EMD and RFP Document Fees are found in order, shall be considered for Pre-Qualification criteria evaluation.

b) Bidder shall be evaluated as per prequalification criteria mentioned in the RFP. The bidders who fulfil all the Pre-Qualification criteria will qualify for further Technical Evaluation.

5.33.4. Evaluation of Technical Proposals

The evaluation of the Technical Proposals will be carried out in the following manner:

- The Bidders' technical solution will be evaluated as per the requirements and evaluation criteria as spelt out in the RFP document. The Bidders are required to submit all required documentation in support of the evaluation criteria specified (e.g. detailed Project citations and completion certificates, client contact information for verification, profiles of Project resources and all others, etc.) as required for technical evaluation.
- The Bidder should cover scope of work, complexity of implementation, and critical success factor as specified in the evaluation section.
- At any time during the tender evaluation process, the Committee may seek verbal / written clarifications from the Bidders. The primary function of clarifications in the evaluation process is to clarify ambiguities and uncertainties arising out of the evaluation of the Bid documents. Verbal / Written clarifications provide the opportunity for the Committee to state its requirements clearly and for the Bidder to more clearly state its Proposal. The Committee may seek input from their professional and technical experts in the evaluation process.
- MH Cyber Department reserves the right to do a reference check of the experience stated by the Bidder. Any feedback received during the reference check shall be considered during the technical evaluation process.
- Proposal Presentation: Proposal Presentation would be evaluated for clarity, design, timelines, team structure, proposed solution etc.

5.33.5. Technical Evaluation Methodology

- Each Technical Proposal will be assigned a Technical Score out of a maximum of 100 points.
- To qualify for the opening of Commercial Proposal, the Bidder must get a minimum overall Technical Score of 70 out of 100.
- The Commercial Proposals of Bidders who do not qualify technically shall be kept unopened in the e-Tendering system.
- The Committee shall indicate to all the Bidders the results of the Technical Evaluation through a written communication. The Technical Scores of the Bidders will be announced prior to the opening of the Commercial Proposals.
- The technically shortlisted Bidders will be informed of the date and venue of the opening of the Commercial Proposals through email or written communication.

5.33.6. Evaluation of Commercial Proposals

The MH Cyber Department will open the Commercial Bids of only the technically qualified MH Cyber Department, in the presence of the representatives of the Bidders who choose to attend, at the time, date and place, as decided by the MH Cyber Department.

The Commercial Bids will be opened and compared (after the technical evaluation is completed) for those Bidders whose technical bids reach the minimum threshold standards (i.e., 70 marks).

Bidder "Scoring highest as per QCBS Process" will be considered for as successful bidder.

5.33.7. Selection of bidder

The bidder whose quote is lowest will be considered as successful bidder.

5.34. Award of Contract

5.34.1.Right to accept and to reject any Proposal

MH Cyber Department reserves the right to accept or reject any Proposal, and to annul the tendering process and reject all Proposals at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for MH Cyber Department action.

5.34.2.Notification of Award

Prior to the expiration of the validity period, MH Cyber Department will notify the Successful Bidder that its Proposal has been accepted by issuance of a Letter of Acceptance in writing or through email. Until a formal contract is prepared and executed, Letter of Acceptance shall constitute a binding Contract.

5.34.3.Performance Bank Guarantee

A PBG of **3% of contract value** would be furnished by the successful Bidder as per the format provided in the RFP document from Nationalized/Scheduled Bank. The PBG should be furnished within 15 Business Days from the date of issue of Letter of Acceptance and should be valid for period of 180 days over and above the Contract Period.

5.34.4.Signing of Contract

MH Cyber Department shall have the right to annul the award in case there is a delay of more than 30 days in signing of Contract from the date of issue of Letter of Acceptance by MH Cyber Department, for reasons attributable to the successful Bidder. Bidder must register the contract within 15 days of signing of contract.

The successful Bidder is required to execute a contract agreement in the pro-forma attached with the Bid documents on stamp paper of appropriate value as per Maharashtra Stamp Act, 1958 (as amended from time to time). The contract agreement should be executed within 30 days from the date of receipt of acceptance letter.

RFP, Corrigenda, Request for Clarifications issued, Technical Proposal, any clarifications received, Presentations, etc. made by the 'successful Bidder' during the Bid evaluation phase will form part of the Contract signed with the Bidder.

5.34.5.Failure to agree with Terms and Conditions of this RFP

Failure of the successful Bidder to agree with the terms & conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event MH Cyber Department may call for new Proposals and invoke the Performance Bank Guarantee (PBG).

6. Scope of Work

6.1. Overview

The MahaCyber Safe Mobile Application is a proposed initiative to provide a centralized, mobile-based cybersecurity awareness and protection platform for citizens of Maharashtra. The application is intended to offer real-time security insights, threat identification, and proactive risk mitigation through an easy-to-use mobile interface. It will integrate multiple cybersecurity features to help users assess and manage digital risks associated with mobile usage. The solution will include a citizen-facing mobile application supported by a centralized administrative system for monitoring and management. The platform aims to improve cyber awareness, enable informed decision-making, and strengthen the overall cyber safety ecosystem. The project is aligned with the objectives of Maharashtra Cyber Department to enhance citizen safety in the digital domain.

6.2. Project Objectives

The objectives of the MahaCyber Safe Mobile Application project are as follows:

- To develop and deploy a mobile-based platform that provides cybersecurity awareness and protection services to citizens of Maharashtra.
- To enable citizens to identify potential cyber threats through real-time scanning, alerts, and security assessment features.
- To promote safe digital practices by providing timely cyber advisories, awareness updates, and actionable recommendations.
- To establish a centralized system for monitoring application usage, managing cybersecurity content, and generating analytical reports.
- To support informed oversight by authorized government authorities through access to system-level dashboards and analytics.
- To ensure accessibility and usability of cybersecurity services through a user-friendly mobile application.
- To strengthen the overall cyber safety ecosystem by enabling proactive identification and mitigation of digital risks.

6.3. Detailed Scope of Work

6.3.1. Phase 1: Requirement Gathering and Analysis

The SI shall undertake comprehensive requirement gathering in consultation with Maharashtra Cyber Department and other designated stakeholders. This phase shall include:

- Conducting stakeholder workshops and requirement discovery sessions.
- Understanding existing processes, cybersecurity initiatives, and operational workflows.
- Identifying functional, non-functional, security, performance, and compliance requirements.
- Preparing detailed documentation including Functional Requirement Specification (FRS) and System Requirement Specification (SRS).
- Establishing requirement traceability to ensure alignment between business needs and system functionalities.
- Incorporating stakeholder feedback and obtaining formal approval and sign-off before proceeding to the design phase.

6.3.2. Phase 2: Solution Design and Architecture

Based on approved requirements, the SI shall design a robust, scalable, and secure system architecture. This phase shall include:

- Preparation of High-Level Design (HLD) covering overall architecture, system components, integrations, and deployment model.
- Preparation of Low-Level Design (LLD) detailing module-level design, workflows, data structures, interfaces, and security controls.
- Defining user roles, access rights, audit mechanisms, and data flow.
- Ensuring compliance with scalability, interoperability, performance, and security considerations.
- Submission of design documents for review, revisions, and formal approval by the competent authority.

6.3.3. Phase 3: Application Development and Integration

The SI shall develop the solution strictly in accordance with approved designs and specifications. The scope includes:

- Development of the citizen-facing mobile application with approved cybersecurity functionalities.
- Development of the web-based administrative application for configuration, monitoring, reporting, and content management.
- Implementation of backend services and secure RESTful APIs for system communication.
- Integration of approved third-party or external services, where applicable.
- Implementation of role-based access control, logging, and audit trail mechanisms.
- Adoption of secure coding practices and standard development methodologies.

6.3.4 Phase 4: Testing and Quality Assurance

The SI shall ensure comprehensive testing and quality assurance before deployment. This phase shall include:

- Preparation and submission of a detailed Test Plan and Test Cases.
- Execution of unit testing, system testing, integration testing, performance testing, and security testing.
- Identification, tracking, and resolution of defects.
- Support for User Acceptance Testing (UAT) conducted by the department.
- Incorporation of UAT feedback and submission of final builds.
- Obtaining formal UAT sign-off prior to deployment.

6.3.5 Phase 5: Deployment and Go-Live

Upon successful completion of testing, the SI shall undertake controlled deployment activities, including:

- Preparation of a detailed deployment and rollout plan.
- Deployment of the mobile application and administrative system in the approved production environment.
- Configuration and validation of system components post-deployment.
- Support for publishing the mobile application on authorized distribution platforms, where applicable.
- Final system verification and stabilization.
- Obtaining formal Go-Live approval from the department.

6.3.6 Phase 6: Training and Knowledge Transfer

The SI shall ensure operational readiness through:

- Training sessions for designated administrators and operational staff.
- Provision of user manuals, administrator guides, and technical documentation.
- Knowledge transfer sessions covering system operation, configuration, and maintenance.

6.3.7 Phase 7: Operations and Maintenance (O&M)

Post Go-Live, the SI shall provide Operations and Maintenance support for the contract duration, including:

- Continuous system monitoring to ensure availability and performance.
- Corrective, preventive, and adaptive maintenance.
- Bug fixes, patches, and approved updates.
- Helpdesk and technical support as per defined service levels.
- Periodic system health checks and performance reporting.

6.3.7.1 Phase 7A: Citizen Support and Assistance Enhancements

The SI shall implement citizen support and assistance mechanisms to ensure effective service delivery, including:

- In-application help and FAQ modules addressing common cyber safety queries and application usage.
- Citizen support request or grievance submission functionality with categorization.
- Tracking and status updates for submitted support requests.
- Configuration of standardized response workflows to ensure consistency and compliance.

6.3.8 Phase 8: Multilingual and Localization Capabilities

The SI shall ensure multilingual accessibility and localization of the application, including:

- Support for Marathi, Hindi, and English languages.
- Dynamic language selection within the application.
- Localization of cyber advisories, notifications, and content.
- Unicode-compliant content management to ensure accurate rendering across languages.

6.3.9 Phase 9: Performance, Reliability, and Monitoring

The SI shall ensure performance, reliability, and operational stability of the solution, including:

- Monitoring of system availability, response times, and resource utilization.
- Graceful error handling and fault tolerance mechanisms.
- Periodic performance tuning and optimization.
- Administrative dashboards for monitoring usage and system health.

6.3.10 Phase 10: Privacy and Trust-Building Measures

- The SI shall incorporate privacy and transparency measures, including:
- Implementation of user consent mechanisms for data collection and notifications.
- Clear visibility of privacy policy and terms of use within the application.
- Data minimization practices aligned with applicable guidelines.
- Secure handling and storage of user data.

6.3.11 Phase 11: Admin and Governance Enhancements

- The SI shall provide governance and administrative features, including:
- Role-based access control for administrative users.

- Content approval and publishing workflows.
- Audit logging of configuration and content changes.
- Reporting and data export capabilities for authorized users.

6.3.12 Phase 12: Security, Compliance, and Audit Support

The SI shall ensure ongoing security and compliance throughout the project lifecycle, including:

- Compliance with applicable Government of India and MeitY security guidelines.
- Implementation and maintenance of security controls, logs, and audit trails.
- Support for security audits, inspections, and compliance reviews.
- Timely remediation of identified security gaps.

6.3.13 Phase 13: Security, Compliance, and Audit Support

The SI shall ensure ongoing security and compliance throughout the project lifecycle, including:

- Compliance with applicable Government of India and MeitY security guidelines.
- Implementation and maintenance of security controls, logs, and audit trails.
- Support for security audits, inspections, and compliance reviews.
- Timely remediation of identified security gaps.

6.3.14 Phase 14: Documentation and Reporting

The SI shall maintain comprehensive documentation and reporting, including:

- Project plans, progress reports, and milestone submissions.
- Operational and maintenance reports.
- Audit and compliance-related documentation as required by the department.
- Monthly Progress Reports (MPR)
- Phase completion reports
- UAT & Go-Live reports
- Risk & issue tracking reports
- MoM for review meetings
- Final system documentation

6.4 Functional Scope

This section defines the detailed functional scope of the MahaCyber Safe Mobile Application and the associated administrative system. The System Integrator (SI) shall design, develop, implement,

test, deploy, and maintain the functionalities listed below strictly in accordance with the approved Technical Presentation.

6.4.1 Citizen Mobile Application – Functional Scope

6.4.1.1. User Access and Account Management

The mobile application shall provide the following user access and account management functionalities:

- User Registration through valid credentials.
- User Login for registered users.
- Guest Login with limited access to application features.
- Email verification during the registration process.
- Password recovery and reset functionality.
- User account management, including password change.
- Access to the application privacy policy.

6.4.1.2 Cyber Threat Detection and Scanning

The application shall include real-time threat detection and scanning capabilities, including:

- QR Code Scanning to extract data such as URLs, payment links, text, or application links and automatically assess associated risks.
- URL Scanning to determine whether a URL is safe or malicious, including identification of phishing, malware, or spam-related threats.
- Wi-Fi Security assessment to display security rating, encryption type, BSSID, and safety status of connected and available Wi-Fi networks.
- Display of visual risk indicators to clearly communicate threat severity to users.

6.4.1.3 Cyber Safety Awareness and Alerts

The application shall provide awareness and alerting features, including:

- Cyber News module delivering real-time cybersecurity alerts, advisories, and awareness updates.
- Display of cyber news with title, summary, date, and reference link.
- Push notifications for cyber alerts, advisories, and security-related information.

6.4.1.4 Identity and Communication Security

The application shall provide identity and communication protection features, including:

- OTP Security functionality to check call forwarding status and disable call forwarding, with confirmation to the user upon successful action.

6.4.1.5 Data Protection and Breach Awareness

The application shall include data protection features, including:

- Data Breach Check functionality allowing users to verify whether an email address has been compromised in known data breaches.
- Display of breach results along with recommended user actions.

6.4.1.6 Device and Application Security

The application shall provide device-level and application-level security features, including:

- App Permissions analysis to list installed applications, requested permissions, and associated risk levels.
- Security Advisor module to assess device-level settings and configurations and display safe or risky status.
- Detection and listing of Hidden Applications installed on the device.
- Adware Scan to identify applications exhibiting adware-related behaviour and recommend corrective actions.
- Threat Analyzer to scan installed applications and classify them as risky or non-risky.

6.4.1.7 Application Usage Insights

The application shall provide usage and analytical insights to users, including:

- App Statistics displaying application usage time, network usage, and update history.

6.4.1.8 Emergency and Safety Feature

The application shall include an SOS feature that triggers an emergency protocol, including sending alerts with GPS location and device details and displaying confirmation to the user.

6.4.1.9 Accessibility and Multilingual Support

The application shall ensure inclusive access and usability, including:

- Multi-language support for Marathi, Hindi, and English.
- Dynamic language selection within the application.
- Text-to-speech functionality to support visually impaired users.

6.4.2 Administrative Web Application – Functional Scope

The SI shall develop a web-based administrative application to support configuration, monitoring, governance, and reporting, including:

- User and role management for administrative and government users.
- Configuration and management of integrated APIs and security services.
- Cyber news and awareness content creation, approval, and publishing.
- Monitoring dashboards displaying usage statistics, trends, and system analytics.

- Access to detailed audit trails covering user activities, administrative actions, and configuration changes.
- Generation and export of reports for authorized government authorities.

6.4.3. Role-Based Functional Access

The system shall support role-based access with clearly defined permissions, including:

- Citizen Users with access to mobile application functionalities.
- Admin Users with access to configuration, content management, monitoring, and reporting features.
- Government Authority Users with access to system-wide reports, analytics, and oversight dashboards.

6.4.4 Cloud Hosting

- Cloud Hosting shall be provided by the department.

7. Project timelines and payment terms

T is date of award of contract

Sr. No.	Service	Activity / Task	Timeline	Payment (% of Total Project Cost)
1	Solution Configuration & Customization	Configuration and customization of the MahaCyber Safe Mobile Application and Administrative Web Portal as per approved functional scope and technical presentation	**T + 30 Days**	**25%**
2	Integration with Security Services & APIs	Integration with required security engines, APIs, notification services, dashboards, and third-party systems as approved by the Department	**T + 45 Days**	**15%**
3	Testing, UAT & Go-Live	System testing, security testing, UAT support, resolution of observations, and Go-Live	**T + 60 Days**	**15%**
4	Training & Knowledge Transfer	Training of designated Department and administrative users, submission of training material, user manuals, and system documentation	**T + 70 Days**	**0%** *(included in O&M scope)*
5	Operations & Maintenance (O&M)	Post Go-Live support, monitoring, incident handling, upgrades, multilingual support, accessibility support, and maintenance of MahaCyber Safe Mobile Application	**Post Go-Live – 5 years**	**45%** *(paid in equal quarterly instalments over the contract period)*

8. Service level agreement

The purpose of service level agreement is to clearly define levels of service that are expected to be provided by the service provider.

Sr. No.	Performance Parameter	Target / SLA Requirement	Measurement Method	Penalty for Non-Compliance
1	Mobile Application Availability	≥ **99.5% per month**	Monthly uptime calculation excluding approved downtime	2% of quarterly O&M payment for up to 0.5% shortfall; 5% for >0.5% shortfall
2	Admin Web Portal Availability	≥ **99.5% per month**	System monitoring logs	Included in availability penalty
3	Critical Incident Response (P1)	≤ **30 minutes**	Incident ticket timestamps	2% of quarterly O&M payment per incident
4	Critical Incident Resolution (P1)	≤ **4 hours**	Incident closure report	3% of quarterly O&M payment per incident
5	High Severity Incident Resolution (P2)	≤ **8 hours**	Incident management system	2% of quarterly O&M payment
6	Medium Severity Incident Resolution (P3)	≤ **24 hours**	Incident logs	1% of quarterly O&M payment
7	Security Patch Deployment (Critical)	≤ **72 hours**	Patch deployment records	3% of quarterly O&M payment
8	Vulnerability Fix (High / Medium)	≤ **7 days**	Security audit reports	2% of quarterly O&M payment
9	QR / URL Scan Response Time	≤ **5 seconds** (95% cases)	Application performance logs	1% of quarterly O&M payment
10	App Screen Load Time	≤ **3 seconds** (95% cases)	Performance monitoring tools	1% of quarterly O&M payment
11	Multilingual Support Availability	Marathi, Hindi, English – **100% availability**	Functional verification	1% of quarterly O&M payment
12	Text-to-Speech Accessibility	**100% uptime**	Accessibility test reports	1% of quarterly O&M payment

13	Citizen Support Availability	**24×7 support**	Support logs and shift records	2% of quarterly O&M payment
14	Citizen Query Response Time	≤ **24 hours**	Ticketing system	1% of quarterly O&M payment
15	Data Breach Reporting	≤ **6 hours** from detection	Incident reporting records	5% of quarterly O&M payment
16	Backup & Data Recovery	Daily backups with successful restore	Backup logs	2% of quarterly O&M payment
17	SLA & Performance Reporting	Monthly / Quarterly reports on time	Report submission records	1% of quarterly O&M payment
18	Repeated SLA Breach	3 consecutive quarters	SLA compliance review	Right to terminate contract

Total penalties shall not exceed 15% of monthly O&M charges, after which the Department may issue a performance warning or initiate corrective actions.

Parameter	Metric	Basis	Penalty
Adherence to planned implementation schedule as mentioned in section 7 of this RFP.	The delay for each milestone as per the planned schedule should not exceed more than a week without a justified reason agreed and approved by MH Cyber department.	Per Occurrence	Rs 10,000 per day of delay.

9. General Terms and Conditions

9.1. Applicable Law

The Contract shall be interpreted in accordance with the laws of the Union of India.

9.2. Taxes and Duties

The successful bidder shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed etc. excluding service tax which shall be paid by MH Cyber Department as actual separately.

9.3. Confidential Information

1. MH Cyber Department and the successful bidder shall keep confidential and shall not, without the written consent of the other party hereto, divulge to any third party any documents, data, or other information furnished directly or indirectly by the other party hereto in connection with the

Contract, whether such information has been furnished prior to, during or following completion or termination of the Contract.

2. The successful bidder shall not use the documents, data, and other information received from MH Cyber Department for any purpose other than the services required for the performance of the Contract.

9.4. Change in Laws and Regulations

Unless otherwise specified in the Contract, if after the date of the Invitation for Bids, any law, regulation, ordinance, order or bylaw having the force of law is enacted, promulgated, abrogated, or changed that subsequently affects the Delivery Date and/or the Contract Price, then such Delivery Date and/or Contract Price shall be correspondingly increased or decreased, to the extent that the successful Bidder has thereby been affected in the performance of any of its obligations under the Contract.

9.5. Force Majeure

1. The successful bidder shall not be liable for termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.
2. For purposes of this Clause, Force Majeure means an event or situation beyond the control of the successful bidder that is not foreseeable, is unavoidable, and its origin is not due to negligence or lack of care on the part of the successful bidder. Such events may include, but not be limited to, act of God, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.
3. If a Force Majeure situation arises, the successful Bidder shall promptly notify MH Cyber Department in writing of such condition and the cause thereof. Unless otherwise directed by MH Cyber Department in writing, the successful Bidder shall continue to perform its obligations under the Contract as far as it is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

9.6. Change Orders and Contract Amendments

1. MH Cyber Department may at any time order the successful bidder to make changes within the general scope of work.
2. If any such change causes an increase or decrease in the cost of, or the time required for, the successful bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or in the Delivery and Completion Schedule, or both, and the Contract shall accordingly be amended. Any claims by the successful bidder for adjustment under this Clause must be asserted within 28 days from the date of the successful bidder's receipt of MH Cyber Department change order.
3. Prices to be charged by the successful bidder for any Related Services that might be needed but which were not included in the Contract shall be agreed upon in advance by the parties and

shall not exceed the prevailing rates charged to other parties by the successful Bidder for similar services.

9.7. Settlement of Disputes

1. If a dispute of any kind whatsoever arises between MH Cyber Department and Bidder in connection with, or arising out of, the Contract or the execution of the Works, whether during the execution of the Works or after their completion and whether before or after repudiation or Foreclosure or termination of the Contract, including any dispute as to any opinion, instruction, determination, certificate or valuation of ADG – Maharashtra Cyber, the matter in dispute shall, in the first place, be referred in writing to ADG – Maharashtra Cyber, with a copy to the other party. Such reference shall state that it is made pursuant to this Clause. Not later than the Ninetieth Day after the day on which he received such reference the ADG – Maharashtra Cyber shall give notice of his decision to MH Cyber Department and Bidder. Such decision shall state that it is made pursuant to this Clause.

9.8. Extensions of Time

1. If at any time during performance of the Contract, the successful bidder should encounter conditions impeding timely delivery of the Services, the successful bidder shall promptly notify MH Cyber Department in writing of the delay, its likely duration, and its cause. As soon as practicable after receipt of the successful bidder's notice, MH Cyber Department shall evaluate the situation and may at its discretion extend the successful bidder's time for performance in writing.
2. Delay by the successful Bidder in the performance of its Delivery and Completion obligations shall render the Bidder liable for disqualification for any further bids in MH Cyber Department, unless an extension of time is agreed mutually.

9.9. Termination

1. If the successful bidder does not remedy a failure in the performance of its obligations under the Contract, within thirty (30) days after being notified or within any further period as MH Cyber Department may have subsequently approved in writing.
2. If the successful bidder becomes insolvent or goes into liquidation, or receivership whether compulsory or voluntary.
3. If the successful bidder, in the judgment of MH Cyber Department has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.
4. If, as the result of Force Majeure, the successful bidder is unable to perform a material portion of the Services for a period of not less than 60 days.
5. If the successful bidder submits to the MH Cyber Department a false statement which has a material effect on the rights, obligations or interests of MH Cyber Department.

6. If the successful bidder places itself in a position of conflict of interest or fails to disclose promptly any conflict of interest to MH Cyber Department.
7. If the successful bidder fails to provide the quality services as envisaged under this Contract, MH Cyber Department may make judgment regarding the poor quality of services, the reasons for which shall be recorded in writing. MH Cyber Department may decide to give one chance to the successful Bidder to improve the quality of the services.
8. If the successful bidder fails to comply with any final decision reached because of dispute settlement committee proceedings.
9. If MH Cyber Department, in its sole discretion and for any reason whatsoever, decides to terminate this Contract.

9.10. Assignment

If successful bidder fails to render services in stipulated timeframe and as per schedule, MH Cyber Department, at its discretion and without any prior notice to successful bidder, may discontinue or minimize scope of work or procure/board any other similar agency to render similar services to complete project in stipulated timeframe.

9.11. Intellectual Property Rights

Ownership of entire source code, documents, APIs etc developed by service provider for this solution shall lie with MH Cyber Department till the entire project duration.

10. Annexures

10.1 Pre-Qualification Cover Letter

(To be submitted on the Letterhead of the Bidder)

To,
The Office of the Additional Director General of Police,
Maharashtra State Cyber,
Home Department,
Mumbai, Maharashtra.

Subject: Submission of Proposal in response to the RFP for
"Appointment of Agency for Design, Development, Deployment, Operations and Maintenance of MahaCyber Safe Mobile Application"

Dear Sir,

Having examined the Request for Proposal (RFP), the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the RFP for the project titled **"Appointment of Agency for Design, Development, Deployment, Operations and Maintenance of MahaCyber Safe Mobile Application."**

We hereby submit our response to the Pre-Qualification requirements along with the Technical and Commercial Proposals, in accordance with the terms and conditions specified in the RFP document. We confirm that the information contained in this proposal, including all annexures, enclosures, and supporting documents, is true, accurate, verifiable, and complete in all respects.

We further confirm that this submission includes all information necessary to ensure that the statements contained herein do not, in whole or in part, mislead Maharashtra State Cyber during the evaluation and selection process.

We fully understand and agree that, in the event any information provided in this proposal is found to be false, misleading, or incorrect at any stage, Maharashtra State Cyber shall have the right to disqualify our bid, cancel the selection, or terminate the contract without any liability, if awarded.

We unconditionally accept all the terms and conditions stipulated in the RFP document and agree to abide by the provisions of this bid for a period of **180 days** from the date of submission of the proposal. We further confirm that, upon award of the contract, we shall furnish the **Contract Performance Guarantee** in the manner and form prescribed in the RFP.

We acknowledge that Maharashtra State Cyber is not bound to accept the lowest or any proposal and reserves the right to reject any or all proposals, wholly or partially, without assigning any reason thereof.

It is hereby confirmed that the undersigned is duly authorized and empowered to sign this proposal on behalf of the bidding organization and to bind the organization to the terms and conditions contained herein, as well as to execute any further documents required in connection with this RFP.

Signature of Authorized Signatory
(With Official Seal)

Name:
Designation:
Name of the Organization:
Registered Address:
Telephone:
Email Address:

10.2 Declaration of not being banned by any Government Organization

(Company letterhead)

To,

The Office of the Additional Director General of Police,

Maharashtra State Cyber,

32nd Floor, Centre - 1, World Trade Centre,

Cuffe Parade, Mumbai - 400005

Dear Sir,

Sub: Declaration of not being banned or debarred by any Government Organization

I, authorized representative of _____, hereby solemnly confirm that the Company ……is not banned by any Government Organization which includes any Government Department, Public Sector Undertakings of the Government, Statutory Boards formed by the Government, Local Bodies in the State, Co-operative Institutions in the State, Universities and Societies formed by the Government for any reason as on last date of submission of the Bid. In the

event of any deviation from the information/ declaration, Maharashtra State Cyber reserves the right to reject the Bid or terminate the Contract without any compensation to the Company.

Thanking you,

Yours faithfully

(Signature of the Authorized signatory of the Bidding organization)

Name :

Designation :

Date :

Time :

Seal :

10.3 Non-Disclosure Agreement

(To be submitted on the Letterhead of the Bidder)

This AGREEMENT (hereinafter referred to as the **"Agreement"**) is made on this **[day]** day of **[month]**, **[year]**, between **Maharashtra State Cyber**, Home Department, Government of Maharashtra, having its office at Mumbai, Maharashtra (hereinafter referred to as **"Maharashtra State Cyber"**), on the one part, and **[Name of the Bidder]**, having its registered office at **[Address]** (hereinafter referred to as the **"Bidder"**), on the other part.

WHEREAS

1. Maharashtra State Cyber has issued a Request for Proposal (RFP) inviting bids for the project titled **"Appointment of Agency for Design, Development, Deployment, Operations and Maintenance of MahaCyber Safe Mobile Application"** (hereinafter referred to as the **"Project"**).
2. The Bidder, having represented to Maharashtra State Cyber that it is interested in participating in the bidding process for the said Project, has requested access to information relating to the Project.
3. Maharashtra State Cyber and the Bidder hereby agree as follows:

AGREEMENT

a) In connection with the Project, Maharashtra State Cyber agrees to provide the Bidder with the Request for Proposal and related documents, which may contain confidential, proprietary, or sensitive

information relating to Maharashtra State Cyber's systems, processes, operations, cybersecurity architecture, and strategic plans (hereinafter referred to as **"Confidential Information"**).
b) The Bidder to whom such Confidential Information is disclosed shall:
i. Hold such Confidential Information in strict confidence and protect it with at least the same degree of care as it uses to protect its own confidential and proprietary information.
ii. Restrict disclosure of the Confidential Information solely to those of its employees, consultants, or agents who have a strict "need to know" for the purpose of bidding for the Project and ensure that such persons are made aware of their confidentiality obligations.
iii. Use the Confidential Information solely for the purpose of preparing and submitting its bid in response to the RFP and for no other purpose whatsoever.
iv. Not copy, reproduce, or otherwise duplicate the Confidential Information, except as strictly required for the purpose of bidding for the Project.
v. Maintain a record of the number of copies made, if any.
vi. Upon completion of the bidding process, and in the event of the Bidder being unsuccessful, promptly return to Maharashtra State Cyber or securely destroy all Confidential Information, including all copies, notes, extracts, and reproductions thereof.

4. The Bidder shall have no obligation to preserve the confidentiality of any information which:
a) Was lawfully known to the Bidder prior to disclosure by Maharashtra State Cyber, as evidenced by written records prepared before such disclosure; or
b) Becomes publicly available through no wrongful act or omission of the Bidder; or
c) Is independently developed by the Bidder without reference to or use of the Confidential Information and without involvement of personnel who had access to such information.

5. This Agreement shall apply to all Confidential Information relating to the Project disclosed by Maharashtra State Cyber to the Bidder, whether orally, visually, electronically, or in writing.

6. Maharashtra State Cyber shall be entitled to seek immediate injunctive relief in the event of any breach or threatened breach of this Agreement, in addition to any other remedies available at law or in equity.

7. Maharashtra State Cyber reserves the right to disclose information received from the Bidder or generated during the bidding process, as required under the **Right to Information (RTI) Act, 2005**, or any other applicable law.

8. Nothing contained in this Agreement shall be construed as granting any license, right, or interest, whether by implication or otherwise, to the Bidder in respect of any intellectual property, proprietary rights, trademarks, patents, copyrights, or confidential materials of Maharashtra State Cyber. All rights, title, and interest in the Confidential Information shall remain vested exclusively with Maharashtra State Cyber.
The Bidder shall not alter, remove, or obscure any proprietary, confidentiality, copyright, or trademark notices appearing on the Confidential Information and shall reproduce such notices on all permitted copies.

9. This Agreement shall come into force on the date of execution and shall remain **valid perpetually**, irrespective of whether the Bidder is selected or not.

10. Upon written demand by Maharashtra State Cyber, the Bidder shall immediately:
i. Cease use of the Confidential Information;
ii. Return or destroy all Confidential Information and copies thereof; and
iii. Certify in writing its compliance with the obligations under this Agreement.

11. This Agreement constitutes the entire understanding between Maharashtra State Cyber and the Bidder concerning the subject matter herein and supersedes all prior oral or written communications. Any amendment to this Agreement shall be valid only if made in writing and signed by authorized representatives of both parties. This Agreement shall not be assigned or transferred by the Bidder without prior written consent of Maharashtra State Cyber.

12. The Confidential Information is provided on an **"As-Is"** basis. Maharashtra State Cyber makes no representation or warranty regarding the accuracy or completeness of such information and shall not be liable for any reliance placed upon it.

13. This Agreement shall be binding upon and inure to the benefit of Maharashtra State Cyber and the Bidder and their respective successors, affiliates, and permitted assigns.

14. This Agreement shall be governed by and construed in accordance with the **laws of India**, and courts at **Mumbai** shall have exclusive jurisdiction.

For and on behalf of the Bidder
Signature: _____
Name of Authorized Signatory:
Designation:
Date:
Time:
Seal:
Business Address:

10.4 Annual Turnover Format

Annual Turnover for last 3 financial years

NAME OF BIDDER:

Annual Turnover Data for the Last 3 Years			
Year	**Amount Currency**	**Exchange Rate**	**Indian National Rupees Equivalent**
Year 1			
Year 2			
Year 3			
Average Annual Turnover			

1. The information supplied shall be substantiated by data in the audited balance sheets and profit and loss accounts for the relevant years and submitted as attachments in respect of the selected Bidder or all partners constituting the selected Bidder.

2. Contents of this form should be certified by Chartered Accountant of the Bidder.

10.5 Net worth Format

Bidder must fill in this form

NAME OF BIDDER:

Sr. No.	Block Year	Financial Data for Previous 3 Years [Indian National Rupees]		
		FY 2022-23	FY 2023-24	FY 2024-25
Net Worth				
Net Profit				

Contents of this form should be certified by Chartered Accountant of the Bidder.

10.6 Commercial Proposal Covering Letter

(To be submitted on the Company Letterhead)

[Date]

To,

The Office of the Additional Director General of Police,

Maharashtra State Cyber,

32nd Floor, Centre - 1, World Trade Centre,

Cuffe Parade, Mumbai - 400005

Subject: Submission of Commercial Proposal in response to the RFP for **"Appointment of Agency for Design, Development, Deployment, Operations and Maintenance of MahaCyber Safe Mobile Application"**

Dear Sir,

We, the undersigned Bidders, having read, examined, and understood in detail all the bidding documents issued in respect of the **Request for Proposal (RFP) for Appointment of Agency for Design, Development, Deployment, Operations and Maintenance of MahaCyber Safe Mobile Application**, do hereby submit our Commercial Proposal to provide the services as specified in the bidding documents bearing RFP No. _____.

Price and Validity

All prices mentioned in our Commercial Bid are in accordance with the terms and conditions specified in the bidding documents. The prices and other terms and conditions of this Bid shall remain valid for a period of **six (6) months** from the date of submission of the Bid.

We confirm that we are an entity registered in India and that the Bid Price (Total Contract Value) quoted in this Commercial Proposal includes all applicable taxes, duties, levies, including income tax and professional tax, as applicable under Indian laws.

The prices quoted by us shall remain firm and fixed for the entire duration of the Contract and shall not be subject to any escalation whatsoever. Any increase or decrease in applicable taxes, duties, or statutory levies during the contract period shall be borne by us. We have examined the clauses relating to Indian taxation and hereby declare that any change in income tax, surcharge, professional tax, or any other corporate tax shall be paid by us as per applicable laws.

Bid Price Declaration

We declare that the Bid Prices quoted by us are for the **entire scope of work**, including all deliverables, services, and obligations as specified in the RFP documents, irrespective of any statement made elsewhere in our Bid.

Performance Bank Guarantee

We hereby declare that, in the event the Contract is awarded to us, we shall submit the **Performance Bank Guarantee (PBG)** in the form, value, and within the timelines prescribed in the RFP.

We further declare that this Bid has been submitted in good faith, without any collusion, fraud, or misrepresentation, and that the information contained in this Bid is true and correct to the best of our knowledge and belief.

We understand that this Bid shall be binding upon us and that Maharashtra State Cyber is not bound to accept the lowest or any Bid received.

We also confirm that **no technical deviations** have been submitted along with this Commercial Proposal.

Yours faithfully,

Authorized Signatory

Name:
Designation:
Date:
Time:
Seal:
Business Address:

10.7 Commercial Bid Format

a) Total Cost (Summary)

Sr. No	Item	Total Cost exclusive of GST
1	Development and customization of MahaCyber Safe Mobile Application.	
2	Integration with necessary applications	
3	UAT and Go-Live	
4	Training to required number of resources	
5	Support and maintenance for five-year post Go-Live	
	Total Cost in Words ₹	

10.8 Indicative Requirement & Utility of Solution

The need for the Maharashtra Cyber Safe App arises from the rapidly growing threat landscape in Maharashtra, where citizens are increasingly targeted by phishing links, malicious QR codes, Wi-Fi spoofing, OTP hijacking, and data breaches. Existing awareness campaigns and helplines often provide reactive support, but there is a critical gap in proactive, citizen-centric digital protection. With

smartphones being primary medium for digital payments, communication, and e-governance services, a mobile-first security support. By equipping users with accessible tools to detect threats, monitor personal data exposure, and receive verified cyber advisories, the application directly supports Maharashtra Cyber's mission of reducing cybercrime incidents and enhancing public cyber hygiene.

Current Challenges/Gaps

- Rising phishing and malware attacks via QR codes, malicious links, and fake apps.
- Citizens unaware of compromised credentials/data breaches.
- OTP hijacking and SIM swap frauds in financial crimes.
- Lack of a centralized mobile tool to provide both awareness and protection.

Objectives of the Proposed Application

	Overview
Feature	**Details**
Platform	Android and iOS (Cross Platform - Flutter)
Licensing Model	Onetime purchase with 4 years O&M
Overview	• **Description:** A citizen-facing mobile application that provides cybersecurity awareness and protection services, including QR/URL scanning, Wi-Fi security, OTP protection, data breach checks, app permission monitoring, and real-time cyber news. • **Category:** Cybersecurity / Utility • **Target Audience:** Citizens of Maharashtra (public, businesses, students)

- Provide real-time threat detection directly to citizens.
- Enable self-check of compromised accounts, devices, and applications.
- Establish a scalable digital outreach mechanism for cyber hygiene.
- Assist Maharashtra Cyber in proactive citizen protection.

Utility for Cyber Office Operations

- Reduced complaint inflow by preventing incidents.
- Enhanced outreach of cyber awareness initiatives.
- Centralized dashboard for authorities to monitor emerging cybercrime trends.

Use Case

- Citizen scans a suspicious payment QR code →app flags as phishing → prevents fraud
- User checks if their Aadhaar-linked email has been in a breach → alerts them to change credentials → reduces identity theft complaints.
- Law enforcement can broadcast urgent cyber advisories directly on citizens' devices.

10.9 Indicative Scope and Functionality

Category	Details
S	• Coverage: Entire state of Maharashtra, scalable to pan-India. • Target Users: General citizens, businesses, students. • Departments: Maharashtra Cyber, LEAs, CERT-In coordination.
Utility for Cyber Office Operations	• Reduced complaint inflow by preventing incidents. • Enhanced outreach of cyber awareness initiatives.

Category	Details
	• Centralized dashboard for authorities to monitor emerging cybercrime trends.
Modules/Components Included:	• QR/URL Threat Scanner • WiFi Security Scanner • OTP Forwarding Protection • Data Breach Checker • Cyber News Feed & Advisories • App Permission Monitor • Security Advisor (Root/encryption check, hidden apps detection) • Admin Dashboard (Govt. & LEA access)
Workflow and Process Flow	• User initiates scan → App integrates with backend API → Result displayed with risk rating → Citizen receives recommendations → Option to share/report threats with authorities.
Technology Stack Used	• **Frontend:** Flutter (Dart) • **Backend:** ReactJS, .NET Core 7 (Web API) • **Database:** MS SQL Server 2022 • **APIs:** VirusTotal, APIVoid, XposedOrNot, Cyber News API, Telecom USSD Services • **Security:** Token-based authentication, HTTPS, AES-256 encryption
Scalability and Expansion Possibilities	• Expand to include Digital Payment Fraud Tracker, SIM Swap Detector. • Integration with CERT-In threat feeds. • Multi-language UI (Marathi, Hindi, English). • Possible SaaS extension for corporates.
Security Features	• Multi-factor authentication • Encrypted local storage for scan history • TLS 1.3 secure communications • Secure coding practices

10.10 Indicative Technical Specifications

Specification Category	Requirement Details
Hardware Requirements	• **Servers:** Cloud/Govt. Data Center, 8-core CPU, 32 GB RAM, 2 TB SSD. • **User Devices:** Android (10 and above), iOS (14 and above).
Software/OS compatibility	• **Mobile:** Android & iOS smartphones/tablets. • **Server:** Windows/Linux backend hosting.
Security Standards Compliance	• ISO 27001 (Information Security) • NIST Cybersecurity Framework alignment • CERT-In advisory compliance • OWASP MASVS & OWASP Mobile Top 10

Specification Category	Requirement Details
Performance Benchmarks	• **App size:** 70-90 MB • **Startup Time:** < 5 sec • **Threat scan:** 3-5 sec under normal connectivity
Integration with Existing system	• It shall seamlessly integrate with existing system.