

Request for Proposal

for

Information Security Audit & Performance Testing

by

CERT-In Empaneled Agencies

Dated: December 06, 2024

Department of Posts

Ministry of Communications

Government of India

Notice Inviting Tenders

To,

All CERT-In Empanelled Agencies

Subject: Tender for conducting the Information Security Audit and Application Performance testing of DoP Applications under IT 2.0

1. The Department of Posts (*DoP*), Ministry of Communications, Government of India, is undertaking the IT 2.0 Modernization initiative aimed at developing new applications as part of a technology upgrade.
2. To ensure the security and performance of these applications, DoP intends to onboard a CERT-In empanelled information security auditing agency to conduct a comprehensive Information Security Audit and Performance Testing of its applications. This initiative aims to ensure the security, resilience, and optimal performance of DoP's applications, which are critical to its broad range of services, including postal, banking and insurance-related offerings. This document outlines the terms of reference for the engagement, including the scope of work, deliverables, and other requirements.
3. The bids will be opened on the same as per the date / time mentioned in the Important Date Section / GEM portal at the Department of Posts, Dak Bhawan, New Delhi in the presence of bidders who may wish to be present, either by themselves or through their authorized representatives.
4. The detailed Terms & Conditions as Annexure-1, Scope of Work as Annexure 2, Format for submitting Price bid as Annexure-3 and Bidder Details as Annexure-4 are attached with this tender document and can be downloaded from DoP website <https://www.indiapost.gov.in> as well as the GeM portal. (www.gem.gov.in)

Assistant Director General (PMU Division)

Dated: December 06, 2024

Important Dates

S.No	Particulars	Timeline
1	RFP Issuance Date	6 th December, 2024
2	RFP Coordinator Contact details	Assistant Director General (ADG), PMU Division, Department of Posts, Dak Bhawan, Sansad Marg, New Delhi: 110001 Email : adgpmu@indiapost.gov.in
3	Last Date of Written request for Clarifications Before the Pre-bid Meeting	1700 Hrs on 11.12.2024
4	Pre-bid Meeting details (online)	1500 Hrs - 12 th December, 2024 Meeting link ID: 7571490712 Password: 684860 Join Meeting https://bharatvc.nic.in/join/7571490712
5	Last Date of Bid Submission.	1800 Hrs - 26 th December, 2024
6	Technical Bid Opening Date	1830 Hrs - 26 th December, 2024
7	Commercial Bid Opening	The commercial bids of only those Bidders who qualify in both eligibility and technical evaluation will be opened. The date for opening of the commercial bid would be communicated separately to the technically eligible Bidders.
8	EMD	Amount of 60 lakhs to be deposited in the account through NEFT as per details valid for 45 days beyond bid validity date: Account No: 31702160955 Account Name: SENIOR POSTMASTER, SANSAD MARG HO (Receipt A/c) IFSC Code: SBIN0000691 Branch Name: STATE BANK OF INDIA, NEW DELHI MAIN BRANCH,11, PARLIAMENT STREET, NEW DELHI Branch Code: 691

Annexure 1 – Terms & Conditions

1. The applications are to be hosted on the NIC Meghraj cloud so the security audit certificate should comply with the NIC standards. The bidders may well acquaint themselves with NIC standards before applying for tender.
2. The bid shall be submitted in two parts
 - a. Technical Bid for Information Security Audit and Performance Testing of DoP Applications
 - b. Commercial Bid for Information Security Audit and Performance Testing of DoP Applications
3. All pages of the bid being submitted must be signed with the official seal.
4. **Period of Bid Validity:** Bids shall remain valid for 180 days from the date of Bid Opening. Any Bid valid for a shorter period than the period specified shall be rejected as nonresponsive.
5. **Last date & Time for receipt of Bids:** The last date for receipt of Bids is 26th December 2024, till 15:00 Hrs. Bids will be opened on the same day at 15:30 Hrs.
6. **Late Bid:** Any Bid received by the DoP after the deadline for submission of Proposals prescribed in the RFP or Corrigendum shall not be accepted and will not be considered for any further evaluations. Only online Bids that are submitted as per the prescribed time and format shall be accepted. Bid submitted by any other means including, email, hardcopy, Fax etc. shall be rejected.
7. **Language of Bids:** The Bids prepared by the Bidder and documents relating to the bids exchanged by the Bidder and DoP, shall be written in the English language, provided that any printed literature furnished by the Bidder may be written in another language so long as the same is accompanied by an English translation in which case, for purposes of interpretation of the bid, the English version shall govern.
8. **Bid Prices:**
 - a. The prices shall be quoted in Indian Rupees only.
 - b. All taxes, duties, levies applicable etc. shall be indicated clearly.
 - c. Prices quoted must be final and shall remain constant throughout the period of validity of the bid and shall not be subject to any upward modifications, whatsoever.
 - d. Bidders shall indicate their rates in clear/visible figures as well as in words and shall not alter/overwrite/make cuts in the quotation.
9. **Bid Evaluation:**
 - a. During the Eligibility Criteria Evaluation, the bidder's details shall be evaluated against the required Eligibility Criteria as mentioned in this tender document and subsequently, the bids of only eligible bidders shall be considered for final evaluation.

- b. The selection will be made on the basis of Least Cost Based selection method (LCBS)
- c. The bidders are required to score a minimum of 70 Marks in technical evaluation for qualifying for Commercial Bid opening.
- d. Proposals will finally be ranked according to their financial scores
- e. The price bids shall be evaluated as under:
 - i. If there is any discrepancy between words and figures, the amount in words will prevail.
 - ii. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected.
- f. If the Bidder does not accept the correction of the errors as above, the bid shall be rejected.
- g. The bidder whose Financial Bid is the Lowest, shall be considered for the award of the contract for conducting an Information Security Audit and Performance Testing of DoP's Applications.

10. **Work Period:** The work period shall be for 5 years from the date of issue of the Work Order extendable by 2 years on annual basis based on same terms and conditions.

11. Earnest Money Deposit

- a. The Bidder's shall deposit an EMD amount of 60 lakhs in the account through NEFT as per details valid for 45 days beyond bid validity date:
- b. EMD will be accepted through online payment (RTGS/NEFT) to the beneficiary account the details of which are mentioned below:

Account No : 31702160955
 Account Name : SENIOR POSTMASTER, SANSAD MARG HO (Receipt A/c)
 IFSC Code : SBIN0000691
 Branch Name : STATE BANK OF INDIA, NEW DELHI MAIN BRANCH, 11, PARLIAMENT STREET, NEW DELHI
 Branch Code : 691

- c. EMD in any other form will not be accepted
- d. EMD must remain valid for 45 (Forty-Five) days beyond the final bid validity period. The validity of the EMD will be extended in the event the last date of submission of the Proposal is extended. No interest will be payable by DoP on the EMD.

- e. The EMD is required to protect DoP against the risk of Bidder's conduct which may warrant EMD's forfeiture according to the instances mentioned in clause (j) below.
- f. EMD shall be exempted for Government bodies/PSU, SSI and MSE organizations (who are exempted from payment of EMD) on the production of the relevant certificate as proof. The exemption clause, however, does not apply when such Bidder's participate in the Bid Process with private players.
- g. EMDs of all unsuccessful Bidder's will be returned, without interest, at the earliest after the expiry of the final bid validity and latest on or before the 30th day after the award of the contract. However, in case of two packet bidding, the EMD of unsuccessful Bidder's during the first stage i.e., technical evaluation should be returned within 30 days of the declaration of results of the first stage.
- h. The EMD of the successful Bidder will be returned, without interest, upon submission of the Performance Bank Guarantee by the successful Bidder.
- i. In case the EMD is not received by the stipulated deadline, then DoP reserves the right to reject the Proposal of the concerned Bidder forthwith and summarily without providing any opportunity for any further correspondence by the concerned Bidder.
- j. The EMD may be forfeited:
 - i. If a Bidder withdraws the proposal or increases the quoted prices after the opening of the Proposal and during the period of the Bid validity period or its extended period, if any.
 - ii. If the Bidder has its bid withdrawn during the period of bid validity specified by the Bidder on the Bid Form; or
 - iii. If the Bidder, having been notified of the acceptance of its bid by DoP during the period of validity of bid: (a) Withdraws its participation from the bid during the period of validity of bid; or (b) Fails or refuses to participate in the subsequent bid process after having been short listed.
 - iv. In case of a successful Bidder, if the Bidder fails to sign the Agreement per the terms and conditions (including timelines for execution of the Agreement) of this RFP or fails to furnish the Performance Bank Guarantee per the terms and conditions (including timelines for furnishing PBG) of this RFP.
 - v. If the Bidder is found indulging in any corrupt, fraudulent or other malpractice in respect of the bid.
 - vi. During the Bid process, if the Bidder indulges in any act that would jeopardize or unnecessarily delay the process of bid evaluation and finalization.
 - vii. The decision of the DoP regarding the forfeiture of the EMD shall be final and binding on the Bidder's and shall not be called upon in question under any circumstances.

12. Performance Bank Guarantee

- a. The successful Bidder shall at his own expense, deposit with DoP within 14 calendar days of the letter of award (done through the issuance of the Letter of

Acceptance) an unconditional and irrevocable and continuing Performance Bank Guarantee

- b. PBG can be furnished through online payment (RTGS/ NEFT) to the beneficiary account, the details of which are mentioned below:

Account No: 31702160955
Account Name: SENIOR POSTMASTER, SANSAD MARG HO (Receipt A/c)
IFSC Code: SBIN0000691
Branch Name: STATE BANK OF INDIA, NEW DELHI MAIN BRANCH, 11,
PARLIAMENT STREET, NEW DELHI
Branch Code: 691

- c. This PBG will be an amount equivalent to 5% of the contract value (excluding GST). All charges whatsoever such as premium, commission, etc. concerning the security shall be borne by the Bidder. This PBG shall remain valid from the date of execution of the contract to the expiry of 60 calendar days after the date of completion of all contractual obligations including warranty obligations.
- d. The PBG may be discharged/ returned by DoP upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on this amount.
- e. In the event of the selected bidder being unable to service the contract for whatever reason, DoP would invoke the deposit. Notwithstanding and without prejudice to any rights whatsoever of the department under the Contract in the matter, the proceeds of the deposit shall be payable to the department as compensation for any loss resulting from the selected bidder's failure to complete its obligations under the Contract. The department shall notify the selected bidder in writing of the exercise of its right to receive such compensation within 15 calendar days, indicating the contractual obligation(s) for which the selected bidder is in default.
- f. The PBG may be invoked by DoP in the following non-exhaustive events:
- i. If the successful Bidder fails to meet the overall penalty condition as mentioned in the RFP or any changes agreed between the parties after contract signing.
 - ii. If the successful Bidder fails to perform the responsibilities and obligations as set out in the RFP to the complete satisfaction of DoP.
 - iii. If the successful Bidder misrepresents facts/information submitted to DoP.

13. Payment Terms:

- a. Payment will be released after successful completion of respective work for one-time audits and CRs whenever undertaken in each of the respective years, submission of necessary certificate /documents / Report to DoP.
- b. No advance payment shall be made.
- c. No claim on account of any price variation/escalation shall be entertained.
- d. No claim for interest in case of delayed payment will be entertained by the Authority.

14. Service Level Agreement

S.No	Description	Expected Service Levels	Penalty level in case of breach of the expected service level	Base Amount for Calculation
1	Security Breach (For the purposes of this clause, a security breach would be defined as any attack upon DoP system which has been successful)	No Security Breach Incident	5% of payment charges (in respect of security audit and performance testing agency) for the relevant year/s, if it is established through artefacts/investigations and/or audit by DoP appointed external auditor that a security breach could have been avoided if caught by security audit and performance testing team. <i>Exception:</i> In case of security breach under DPDP 2023 Act, Fine/ Penalty as defined under the Act shall be applicable.	The total amount paid to be the bidder for that year including annual audits and regular audits for each change
2	Application Performance Issues (For the purposes of this clause, an application performance would be defined as any degradation of service in accessibility with regards to increased Load/Stress/Spike	No degradation of Service	5% of payment charges (in respect of security audit and performance testing agency) for the relevant year/s, if it is established through artefacts/investigations and/or audit by DoP appointed external auditor that a service degradation could have been avoided if caught by security audit and performance testing team	The total amount paid to be the bidder for that year including annual performance testing and regular performance testing for each change
3	Completion of deliverables under Security Audit and	100% on time	0.5% per day of amount that would have been payable for	The amount payable for the assignment for which the delay has happened

	Performance Testing Agency		the assignment not completed in time	
--	----------------------------	--	--------------------------------------	--

Penalties shall be capped to 10% of the annual payment of the total contract value.

15. DoP’s right to accept or reject any or all bids

DoP reserves the right to accept or reject any Bid, and to annul the Bidding process and reject all Bids at any time before the 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.

16. Conflict of Interest

All bidders shall have to abide by the Code of Integrity detailed in the Tender Document. A bidder shall not have conflict of interest which can lead to anticompetitive practices to the detriment of DoP’s interests. All bidders found to have a conflict of interest shall be disqualified.

- a. Conflicting Bidding: A bidder may be considered to have a conflict of interest with one or more parties in this tender process, if:
 - i. directly or indirectly controls, is controlled by or is under common control with another Bidder; or
 - ii. receives or have received any direct or indirect subsidy/ financial stake from another bidder; or
 - iii. has the same legal representative/ agent as another bidder for purposes of this bid.
 - iv. A Principal can authorize only one agent, and an agent also should not represent or quote on behalf of more than one Principal; or
 - v. has a relationship with another bidder, directly or through common third parties, which puts it in a position to have access to information about or influence the bid of another Bidder or influence the decisions of the Procuring Entity regarding this Tender process; or
 - vi. participates in more than one bid in this tender process. Participation in any capacity by a Bidder (including the participation of a Bidder as sub-contractor in another bid or vice-versa) in more than one bid shall result in the disqualification of his bid as the main/ principal/ lead bidder. However, this does not limit the participation of a non-bidder firm as a sub-contractor in more than one bid; or
 - vii. In case of a holding company having more than one independently manufacturing units, or more than one unit having common business ownership/management, only one unit should quote. Similar restrictions would apply to closely related allied firms. Bidders must proactively declare such allied/ common business/ management units in same/ similar line of business.
- b. Conflicting Activities: would be providing goods, works, or non-consulting services resulting from or directly related to consulting services that it provided (or were provided by any allied firm that directly or indirectly controls, is controlled by, or is under common control with that firm), for the procurement planning (inter-alia preparation of feasibility/ cost estimates/ Detailed Project Report (DPR), design/

- technical specifications, Services and Activities Schedule)/ schedule of requirements or the Tender Document etc.) of this Tender process; or
- c. **Conflicting Relationship:** has a close business or family relationship with a staff of the DoP who: (i) are directly or indirectly involved in the preparation of the Tender document or specifications of the Tender Process, and/or the evaluation of bids; or (ii) would be involved in the implementation or supervision of resulting Contract unless the conflict stemming from such relationship has been resolved in a manner acceptable to DoP throughout the Tender process and execution of the Contract.

17. Force Majeure

- a. "Force Majeure" means an event beyond the control of the Auditor not involving the Auditor's fault or negligence and not foreseeable. This type of event may include but is not limited to fires, explosions, floods, earthquakes, strikes, wars or revolutions etc.
- b. The work execution period may be extended in case of Force Majeure condition. To be able to obtain an extension to the contract work period, the Auditor shall promptly notify the auditee advising the existence of such an event, not later than one week after such an event happens and produce the necessary documents such as a Certificate of Chamber of Commerce or any other competent authority indicating the scope of such an event, and its impact on the performance of the contract and establish that such an event is not attributable to any failures on its part.
- c. **Laws governing contract:** The contract shall be governed by the laws of India for the time being in force.
- d. **Jurisdiction of courts:** The courts of Delhi shall alone have the jurisdiction to decide any dispute arising out of or in respect of the contract.

18. Arbitration:

- a. In the event of any dispute arising out of this notice inviting tender or any agreement arising therefrom or any matter connected or concerned with the said agreement in any manner of its implementation or any terms and conditions of the said agreement, the matter shall be referred to Secretary (Posts), DoP, who may himself/herself act as sole arbitrator or may nominate an officer of DoP as sole arbitrator, even though such officer has been directly or indirectly associated with the agreement. The bidder/ auditor will not be entitled to raise any objection to the appointment of such officer of DoP as the sole arbitrator. The award of the arbitrator shall be final and binding subject to the provisions of the Arbitration and Conciliation Act, 1996 and rules made thereunder. The seat of arbitration shall be in New Delhi, and the language of arbitration shall be in English only.
- b. Arbitration is restricted to dispute with a value less than Rs.10 Crore. This figure is with reference to the value of the dispute (not the value of the contract). Further, it is specifically mentioned here that in all other cases, arbitration will not be a method of dispute resolution.

19. Sub-Contracting

No Subcontracting is allowed in general. However, works related to Performance Testing wherever required may be allowed for sub-contracting subject to approval from DoP and declared as part of the proposal submission with details.

20. Consortium

No consortium is allowed.

21. Limitation of Liability

- a. The liability of the selected bidder (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this RFP, including the work, deliverables or Services covered by this RFP, shall be the payment of direct damages only which shall in no event in the aggregate exceed the Total Contract Value.
- b. The liability of the DoP (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this RFP shall be limited to the amount of fees remaining to be paid to the selected bidder under this RFP.
- c. Except as otherwise provided herein, in no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings), even if it has been advised of their possible existence.

22. Termination

The DoP may, by written notice of 60 (sixty) days sent to the selected Bidder, terminate the Agreement, in whole at any time for its convenience. The notice of termination shall specify that termination is for the DoP’s convenience, the extent to which the performance of work under the Agreement is terminated, and the date upon which such termination becomes effective.

23. Indemnification

The selected bidder (the "Indemnifying Party") undertakes to indemnify the DoP and its nominated agencies (the "Indemnified Party") from and against all losses, claims, damages, compensation etc. on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence, wilful default, lack of due care or breach of terms of this Agreement. The Indemnifying Party shall also indemnify the Indemnified Party from and against all direct monetary losses, damages etc. arising out of any defect, fault, or deficiency in the applications/system/software/solution developed/implemented and or maintained by the Indemnifying Party.

24. Integrity Pact

INTEGRITY PACT

Between

DoP hereinafter referred to as “The Principal”,
and.....hereinafter referred to as “The Bidder/
Contractor”

Preamble

The principal intends to award, under laid down organizational procedures, contract/s for..... The Principal values full compliance with all relevant

laws of the land, rules, regulations, economic use of resources and fairness/transparency in its relations with its Bidder(s)and/or Contractor(s).

To achieve these goals, the principal will appoint Independent External Monitors (IEMs) who will monitor the bid process and the execution of the contract for compliance with the principles mentioned above.

SECTION 1 –COMMITMENTS OF THE PRINCIPAL

(1) The principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

a. No employee of the principal, personally or through family members, will in connection with the bid for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The principal will, during the bid process treat all Bidder(s) with equity and reason. The principal will in particular, before and during the bid process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage concerning the bid process or the contract execution.

c. The principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

SECTION 2 – COMMITMENTS OF THE BIDDER(S)/ CONTRACTOR(S)

(1) The Bidder(s)/ Contractor(s) commits themselves to take all measures necessary to prevent corruption. The Bidder(s)/ Contractor(s) commits themselves to observe the following principles during participation in the bid process and the contract execution.

a. The Bidder(s)/Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the principal's employees involved in the bid process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, to obtain in exchange any advantage of any kind whatsoever during the bid process or the execution of the contract.

b. The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/Contractor(s)will not commit any offence under the IPC/PC Act or such relevant laws, rules, regulations and guidelines; further, the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, all the payments made to the Indian agent/representative have to be in Indian Rupees only.

e. The Bidder(s)/ Contractor(s) will, when presenting their bid, disclose any payments made, are committed to or intend to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f. Bidder(s) /Contractor(s) who have signed the Integrity Pact shall not approach the Courts before and while representing the matter to IEMs and shall wait for their decision in the matter.

(2) The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

SECTION 3 – DISQUALIFICATION FROM THE BID PROCESS AND EXCLUSION FROM FUTURE CONTRACTS

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of SECTION 2, above or in any other form such as to put their reliability or credibility in question, the principal is entitled to disqualify the Bidder(s)/Contractor(s) from the bid process or take action.

SECTION 4 – COMPENSATION FOR DAMAGES

(1) If the Principal has disqualified the Bidder(s) from the bid process before the award according to SECTION 3, the principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to SECTION 3, or if the Principal is entitled to terminate the contract according to SECTION 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

SECTION 5 – PREVIOUS TRANSGRESSION

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the bid process.

(2) If the Bidder makes an incorrect statement on this subject, he can be disqualified from the bid process or action can be taken as per the procedure mentioned in “Guidelines on Banning of business dealings”.

SECTION 6 – EQUAL TREATMENT OF ALL BIDDERS / CONTRACTORS / SUBCONTRACTORS

(1) In the case of Subcontracting, the Principal Contractor shall take responsibility for the adoption of the Integrity Pact by the Subcontractor.

(2) The principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The principal will disqualify from the bid process all bidders who do not sign this Pact or violate its provisions.

SECTION 7 – CRIMINAL CHARGES AGAINST VIOLATING BIDDER(S) / CONTRACTOR(S) / SUBCONTRACTOR(S)

If the Principal obtains knowledge of the conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the principal will inform the same to the Chief Vigilance Officer.

SECTION 8 – INDEPENDENT EXTERNAL MONITOR

The principal has appointed

1. Shri Raj Kumar Singh, IRS (Retd.)

Ex-Member, Customs Excise and Service Tax Appellate Tribunal, New Delhi,
26 Cassia Marg, DLF-2,
Gurgaon – 122008
Tel No.: 0124-4241100
Email ID: mrrajksingh@gmail.com
2. Shri Om Prakash Singh, IPS (Retd.)
Ex-DGP, UP
M-6, Green Park Extension
New Delhi-110016
Ops2020@rediffmail.com

as the Independent External Monitor for this Pact after approval by the Central Vigilance Commission. The details of the appointed IEM are available on the principal's official website. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

(1) The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him/her to treat the information and documents of the Bidders/Contractors as confidential. He/ she reports to the DOP.

(2) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same applies to Subcontractors.

(3) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/Subcontractor (s) with confidentiality. The Monitor has also signed declarations on 'Non-Disclosure of Confidential Information' and of 'Absence of Conflict of Interest'. Notwithstanding anything contained in this Section, the Bidder(s)/Contractor(s) shall have no obligation whatsoever to provide any internal costing mechanisms or any internal financial or commercial data according to any audit or review conducted by or on behalf of the Principal. Further, the Bidder(s)/Contractor(s) shall not be required to provide any data relating to its other DoPs, or any

(4) personnel or employee-related data. The principal will provide the Monitor with sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer the Monitor the option to participate in such meetings.

(5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(6) The Monitor will submit a written report to the DOP within 8 to 10 weeks from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.

(7) If the Monitor has reported to the DOP, a substantiated suspicion of an offence under the IPC/ PC Act and such similar laws, and the DOP has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(8) The word 'Monitor' would include both singular and plural.

SECTION 9 – PACT DURATION

This Pact begins when both parties have legally signed it. It expires for the Contractor, 12 months after the last payment is made under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings. If any claim or discrepancy is made or lodged by any bidder or the principal, during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/determined by DOP.

SECTION 10 – OTHER PROVISIONS

(1) This agreement is subject to Indian Law. The place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to agree with their original intentions.

(5) Issues like Warranty/Guarantee etc. shall be outside the purview of IEMs.

(For & On behalf of the principal) (For & On behalf of Bidder/ Contractor)

Name: Name:

Place: Place:

Date: Date:

Witness1 Witness1:

Address ___ Address _

Witness2 Witness2:

Address Address _____

Annexure 2 – Scope of Work

1. The Auditor is expected to conduct a comprehensive **Information Security Audit** and **Performance Testing** of DoP's applications and carry out an assessment of the vulnerabilities, threats and risks that may exist in the DoP's applications through Vulnerability Assessment and Penetration Testing (*VAPT*) which includes identifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, to enhance the security of the applications.
2. The applications audit should be done by using Industry Standards and as per the Open Web Application Security Project (*OWASP*) methodology and ensuring that application is secure to be granted a safe to host certificate. The audit should be conducted strictly in line with the MeitY guidelines for Cybersecurity Audit available on MeitY's website.
3. List of Tasks to be conducted for Information Security Audit and Performance Testing
 - a. IT Security Policies and Procedures
 - b. Application Security Testing (Web & Mobile) App
 - c. Application/Database Performance Testing
 - d. API Security Assessment
 - e. Network Configuration Assessment
 - f. Cloud Infrastructure Assessment
 - g. Vulnerability Assessment
 - h. Penetration Testing
4. During Security Audit, if any lapse is found, the same shall be reported by the auditor to DoP to make the applications/portal fully secured for hosting on the NIC cloud.
5. DoP's applications are to be hosted on NIC's Meghraj cloud. DoP will provide a staging environment on the NIC cloud for security audit at the time of allotment of work. Bidders are required to share the prerequisites for performing the audit.
6. The audit of the application/portal should be conducted in conformity with NIC audit guidelines. After a successful security audit of the applications, the security audit report from the auditor should clearly state that all web pages along with respective linked data files in (pdf/doc/xls) etc. formats, all scripts and image files are free from any vulnerability or malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said applications.
7. **Audit Environment:** The URL of DoP's Website/Applications to be audited will be shared with the bidder. All the requisite tools/software, and their Supply/installation, if any, for the audit purpose will be the responsibility of the bidder.
8. **Responsibilities of Selected Auditor:** The Selected Auditor will conduct a security Audit for the DoP's applications as under:

8.1. Track 1 – Information Security Audit

8.1.1. Comprehensive Security Audit

Perform a detailed vulnerability assessment and penetration testing of the IT 2.0 applications to identify potential security risks and vulnerabilities, in line with MeitY guidelines for Cybersecurity Audit. *(Refer to Annexure 6 for more details)*

a) Security Policies and Procedures review

Review DoP's existing policies and procedures including, but not limited to, the following:

- i. Security and privacy policy and/ or framework
- ii. Change Management
- iii. Incident Management
- iv. Patch and Release Management
- v. User Access Management
- vi. Vulnerability Assessment and Remediation
- vii. Problem Management
- viii. Risk Assessment
- ix. Backup and Restoration

b) Network Configuration Assessment

Review of Network and Security Architecture along with configuration review, including, but not limited to, the following:

1. WAF
2. IPS/ IDS
3. Firewall
4. SIEM
5. PIM
6. DAM
7. HIDS
8. Proxy

c) Application Security Assessment

1. Conduct static and dynamic application security testing.
2. Comprehensive assessment of the security controls implemented within DoP's applications, including authentication mechanisms, access controls, data encryption, etc.
3. Identification of any vulnerabilities, Injection attacks such as SQL injection, OS command Injections, cross-site scripting (XSS), or insecure direct object references, Cross Site Request Forgery (CSRF), Sensitive data exposure : to ensure with the system comply with National and international data and recommendations for remediation.
4. Review application code for security flaws and weaknesses.
5. Evaluate the security of APIs and security protocols

VAPT should be comprehensive but not limited to following activities:

- i. Injection
- ii. Broken Authentication and Session Management

- iii. Cross-Site Scripting (XSS)
- iv. Insecure Direct Object References
- v. Security misconfiguration
- vi. Insecure Cryptographic Storage
- vii. Sensitive Data Exposure
- viii. Failure to Restrict URL Access
- ix. Missing Function Level Access Control
- x. Cross-Site Request Forgery (CSRF)
- xi. Using Known Vulnerable Components
- xii. Un-validated Redirects and Forwards
- xiii. Insufficient Transport Layer Protection
- xiv. Any other attacks, which are vulnerable to the Applications

d) APIs Security Assessment

1. Conduct security assessment of the APIs, supporting backend Infrastructure and authentication mechanism
2. The assessment shall include testing of up to 500 APIs. The assessment shall be performed on an annual basis.
3. These APIs are designed for all data exchanges within and outside CBIC environment:
 - i. Exchange between two or more applications hosted at NIC Meghraj Cloud
 - ii. Connections with banking and insurance applications of DoP
 - iii. Connections with other government departments/ bodies for data exchange as may be required from time-to-time
4. The assessment shall consider at least the following aspects:
 - i. Data gathering
 - ii. Business logic
 - iii. OWASP based dynamic vulnerability analysis
 - iv. Static analysis of the code

e) Cloud Infrastructure Assessment

Assess the instances of storage, compute and network environments this shall include operating systems and other system software that are outside the boundary of NIC.

VAPT should be comprehensive but not limited to following activities:

- i. Port Scanning
- ii. System Identification & Trusted System Scanning
- iii. Vulnerability Scanning
- iv. Malware Scanning
- v. Spoofing
- vi. Scenario Analysis
- vii. OS Fingerprinting
- viii. Service Fingerprinting
- ix. Password Cracking
- x. Denial of Service (DOS) Attacks
- xi. Authorization Testing
- xii. Lockout Testing
- xiii. Man in the Middle attack
- xiv. Containment Measure Testing

- xv. Server Assessment (OS Security Configuration)
- xvi. Database Assessment
- xvii. Vulnerability Research & Verification
- xviii. Man in the browser attack
- xix. Attempt ARP poisoning
- xx. Attempt MAC flooding
- xxi. Attempt DNS poisoning
- xxii. Any other attacks

f) Penetration Testing

1. Conducting penetration testing activities to simulate real-world attack scenarios and identify potential security vulnerabilities.
2. Reporting on the findings, including exploited vulnerabilities and recommendations for remediation.
3. Recommendations for the remediation and patches for discovered vulnerabilities.

8.1.2. Issuance of “Safe to Host” Certificate

Upon successful remediation of all identified security issues, provide a "Safe to Host" certificate confirming the readiness of the applications for production deployment.

8.1.3. Annual Renewal Audit (VAPT)

Conduct an annual vulnerability assessment and penetration testing (VAPT) to ensure continued compliance with security standards, once every year, for 5 years.

Note: Bidder is required to conduct 2 iterations of Re-Assessment of Information Security after the initial reporting of vulnerabilities.

Bidder may refer to Annexure 6 for MeitY guidelines for Cybersecurity Audit.

8.2. Track 2 –Application Performance Testing

8.2.1. Initial Performance Testing

Test the performance of the IT 2.0 applications to ensure that they support a minimum of 1500 transactions per second (TPS) and handle the required number of concurrent connections without degradation in service quality. *(Refer to Annexure 7 for the definition of a transaction)*

- a) Evaluate system response time, throughput, and resource utilization under peak load conditions.
- b) Identify potential performance bottlenecks and provide recommendations for improvement.
- c) Performance analysis to ensure that the database meets the required response time, throughput, and concurrency demands.
- d) Recommendations for query optimization, indexing strategies, and resource allocation.
- e) Assessment of application and database scalability and high-availability architecture.

8.3. Track 3 –Application Security Assessment for Change Requests

1. Review the SDLC process followed
2. Review of process and system documentations such as SRS, Technical design document, test strategy documents, migration procedures etc. and evaluate compliance to applicable standards
3. Validation of the software development approach against the industry standards
4. Review testing strategies adopted to measure the effectiveness of application functionality coverage and usage of automated testing tools used for functional and non- functional testing
5. Review the change management process, version control and audit trails in application development, testing and production.
6. Review development, testing (RT, SIT, UAT) and production migration and evaluate process compliance to relevant standards
7. Perform Web Application Security Assessment (WASA) of the application, including both authenticated and unauthenticated assessment, based on the best practices including OWASP Top 10. The assessment will check for vulnerabilities, but not be limited to, such as cross-site scripting, SQL injection and privilege escalation.
8. Conduct Security Assessment (automated and manual) for mobile applications (iOS or Android). The tests shall include, but not be limited to, ascertaining that the application
 - i. Does not store sensitive information on external storage (SD card) unless encrypted first
 - ii. Limits accessibility of an app's sensitive content providers
 - iii. Does not allow WebView to access sensitive local resource through file scheme
 - iv. Does not log sensitive information
 - v. Restricts access to sensitive activities
 - vi. Ensures that sensitive data is kept secure

The bidder shall use the 'Business Scenario' based approach involving various business cases /use cases as defined in SRS(s) of the DoP's applications for the information security audit and performance testing. The testing scope will cover all the modules of DoP's applications. This testing will be carried out both through automated tools as well as / scripts manually by executing the test scripts.

9. Deliverables:

The auditor shall deliver the following:

1. **Detailed Security Audit Report:**
 - i. A comprehensive Vulnerable Report detailing the findings, a list of identified vulnerabilities & observations, their severity, and recommendations/mitigation measures/necessary countermeasures and corrective actions to be undertaken by DoP.
 - ii. Clear identification of vulnerabilities, risks, and areas for improvement.
 - iii. Recommendations for remediation, including actionable steps and best practices.
2. **"Safe to Host" Certificate:** Issued after successful completion of the security audit and confirmation that all critical issues have been remediated. The final security audit certificate should comply with the NIC standards.

3. **Performance Testing Report:** Detailing the results of the performance testing, including any performance bottlenecks, their impact, and recommendations for resolution.
 4. **Annual VAPT Report:** A report summarizing the results of the annual vulnerability assessment and penetration testing.
 5. **Revision Audit Report:** A report summarizing the results of the revision audit conducted for performance and testing
10. **Project Milestones:** The audit is expected to be completed as per the following timelines:
1. **M1 - Initial Security Audit and Performance Testing:** Within 8 weeks of onboarding.
 2. **M2 - Subsequent Iterations for Issue Remediation (Security & Performance):** Two iterations after the initial assessment report submission.
 3. **Annual VAPT:** To be conducted within 12 months from the issuance of the "Safe to Host" certificate every year.
 4. **Application Security Assessment and Performance Testing for Change Requests**

S. No.	Milestone	Activity	Timelines
A	M1 (T to T+8 weeks)	Test Scenarios/ Case Design	
A1		Finalize test approach and methodology.	T + 2 weeks
A2		Develop End to End scenarios	T + 3 weeks
A3		Obtain sign-off from DoP.	T + 3 weeks
B		Test Execution	
B1		Obtain the required test environment (Application and Infrastructure) from DoP	T+3 Weeks
B2		Prepare test data	T+3 to T+8 Weeks
B3		Execute test cases	T+3 to T+8 Weeks
C		Test Reporting	
C1		Analyze test observations/ logs.	T+6 to T+8 Weeks
C2		Identify defects/ issues & assign severity/ risk.	T+6 to T+8 Weeks
C3		Prepare defect report of Round 1 and submit it to DoP	T+6 to T+8 Weeks (Weekly)
D		M2 (T+9 to T+16 weeks)	Defect Re-Testing
D1	Carryout re-testing of rectified defects and 2 nd iteration of overall testing		T+9 to T+14 Weeks
D2	Prepare & Issue the final test report.		T+9 to T+14 Weeks
D3	Carryout re-testing of rectified defects and 3 rd iteration of overall testing		T+15 to T+16Weeks
D4	Prepare & Issue the final test report.		T+15 to T+16Weeks

E	M3	Application Security Assessment and Performance Testing for Change Requests	Within 2 weeks from intimation of the Assessment to be conducted and availability of application
E1		Execute test cases	
E2		Analyze test observations/ logs.	
E3		Identify defects/ issues & assign severity/ risk.	
E4		Prepare defect report of Round 1 and submit it to DoP	
E5		Carryout retesting of rectified defects and 2 nd iteration of testing	
E6		Carryout retesting of rectified defects and 3 rd iteration of testing	

11. Application Performance Testing Methodology

Below is the methodology to be used for independent testing of DoP's applications:

11.1. Test Preparation/Design

1. Identification of business functionalities for testing from in-scope modules/interfaces
2. Develop detailed end-to-end business scenarios that will be tested based on
 - a. Most used business scenarios
 - b. Feedback from DoP's users and challenges faced by users
 - c. The top 100 scenarios will be considered. This will be based on consultation with DoP and its stakeholders, and any other criteria as mutually agreed with DoP
3. Develop test cases for identified scenarios which will consist of 4 parts:
 - a. Brief description of the test case
 - b. Pre-requisites
 - c. Steps to be followed
 - d. Expected results

11.2. Testing techniques

1. Scenario testing:
 - a. Test scenarios will be created considering business impact and priority
 - b. For example: A use case related to User Registration/Parcel booking/tracking of consignment may be considered a priority "Critical" use case which will have a severe impact on the DoP's business.
 - c. Thus, priority areas may be "High", "Medium" or "Low" and Impact may be "Severe with material impact", "High with less material impact", "Minor with less/no material impact" and "Negligible with no impact"
2. Equivalence testing:
 - a. Test data is partitioned into equivalence test classes and all data sets in a partition should behave in a similar manner
3. Decision-based testing:
 - a. Various conditions and the expected outcomes are tested. For example: If the user enters the correct details, the system takes the user to the next UI else gives an error message.
4. Boundary value testing:
 - a. It validates the behaviour of the system when tested by applying data limits
5. Alternate flow testing:
 - a. This will validate all possible ways that exist other than the main flow

11.3. Test Execution

1. Obtain the required test environment (H/W & S/W) from DoP and required credentials and 2fa
2. Prepare test data using raw data provided by DoP
3. Execute test cases (SRS/ design documents etc. of each of the core processes needs to be shared by DoP)
4. Verify software functionality in compliance with the specified functional & non-functional requirements as mentioned in the SRS.

11.4. Test Reporting

1. Analyze test observations/ logs
2. Identify defects/ issues & assign severity
3. Prepare defect report of the first round and submit it to DoP
 - a. The defect report will consist of defects due to unsuccessful testing and script errors for automated testing

11.5. Defect Verification & Re-Testing

1. Resolution/ fixing of reported observations within the agreed time frame after the submission of the defect report will be done by the DoP application provider.
2. DoP will validate corrective action on reported defects for closure
3. In case required, perform a second round of testing of rectified defects
4. Prepare & issue the final report
5. Maintain a risk log throughout the lifecycle of the project
6. Provide solution for remediation of the issues reported are due to functional or used software

12. Responsibility of DoP:

- 12.1. The auditor will submit the vulnerability report to the DoP who will be responsible for removing vulnerabilities if any, which are identified by the auditor. After removing the vulnerabilities, DoP will send confirmation to the auditor stating that the vulnerabilities have been removed as mentioned by the auditor.
- 12.2. The reaudits shall be conducted by the auditor after the removal of such vulnerabilities by DoP.
- 12.3. DoP will refrain from carrying out any unusual or major changes during auditing/testing. If necessary, for privileged testing, the auditee can provide necessary access to the Auditor as mentioned in the clause 'Audit Environment' above.

13. Confidentiality: All documents, information and reports relating to the assignment will be handled and kept strictly confidential and not shared/published/supplied or disseminated in any manner, by the Auditor.

14. Technical Details of the applications: Refer to Annexure 6 for the technical details.

Annexure 3 – Bidder's Profile

S. No.	Particulars	Details
1.	Name of the Bidder	
2.	Full Address of the Bidder	
3.	Name & Designation of the Authorized Signatory	
4.	Name & Address of the officer to whom all references shall be made regarding this tender	
5.	Telephone	
6.	Fax No.	
7.	E-mail	
8.	Mobile	

Date _____

Signature: _____

Name: _____

Designation: _____

Company Seal

Annexure 4 – Technical Bid Evaluation

S.No	Parameter	Criteria	Score	Documentary Evidence
1	Number of Audits Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with TPS > 1500	>= 5 and < 10	10	Work Order and Completion Certificate indicating TPS Count
		>= 10	15	
2	Number of Performance Testing Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with TPS > 1500	>= 5 and < 10	10	Work Order and Completion Certificate indicating TPS Count
		>= 10	15	
3	Number of Audits Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with more than 50 Lakhs registered users	>= 5 and <10	5	Work Order and Completion Certificate indicating Number of Users
		>= 10	10	
4	Number of Performance Testing Conducted (Completed) in last 36 months for	>= 5 and <10	5	Work Order and Completion Certificate

	Govt/PSU/Private for each application with more than 50 Lakhs registered users	≥ 10	10	indicating Number of Users
5	No. of technical personnel involved in Information Security Auditing related activities having at least 5 personnel with anyone certification (CEH/ OSCP/ ECSA/ CPTe/ CHFI/ LPT/ CPT/ CEPT/ GPEN/ CMWAPT)	≥ 5 and < 8	5	Self-Certificate with the list of technical personnel indicating total years of experience and experience in Security Auditing Activities
		≥ 8	10	
6	No. of technical personnel under audit agency payroll involved in Performance Testing	≥ 10 and < 20	5	Self-Certificate with the list of technical personnel indicating total years of experience and experience in Performance Testing
		≥ 20	10	
7	No. of technical personnel with CISSP or ISMS (Ex. BS7799/ISO17799/ISO27001) Lead Assessor certification or any other information security qualifications	≥ 2 and < 5	5	Self-Certificate with the list of technical personnel having requisite certifications
		≥ 5	10	
8	Information Security Audit Methodologies	-	10	Detailed Approach & Methodology
9	Performance Testing Methodologies	-	10	Detailed Approach & Methodology

The bidders are required to score a minimum of 70 Marks in technical evaluation for qualifying for Commercial Bid opening.

Annexure 5 – Financial Bid

(On Company Letter Head)

To,

Assistant Director General (PMU Division),
Department of Posts,
Dak Bhawan, Sansad Marg,
New Delhi: 110001

Subject: Financial Bid for Conducting Security Audit of DoP Application

I/We hereby submit the financial bid for conducting a security audit of the DoP Application as per the tender document: -

Description of Work	Frequency	Multiplying Factor	Unit Rate	Amount (Rs.)
One-time Information Security Audit (A)	Once.	1		
One-time Performance Testing (B)	Once.	1		
Information Security Annual Audit (per year cost) (C)	Once every year (for 5 years).	5		
Information Security Audit for application change requests (D)	As per number of change requests	500		
Performance Testing for application change request (E)	As per number of change requests	500		

Taxes (specify) (_____%) (F)		-		
Grand Total [(A) + (B) + (C)+(D) + (E) + (F)]		-		
			Rupees	in
			(Rupees.....)	words
		)	

* For any additional testing to be done above the number predicted for application change request, unit rate shall be used

Note:

- a) The Financial Bid shall contain the quoted Prices only.
- b) Bidders are requested to ensure that this Annexure is duly signed with the company seal. Financial bids submitted without a sign/company seal will not be accepted/considered.

Date_____

Signature: _____

Name: _____

Designation: _____

Company Seal

Annexure 6 – Technical Details of Applications

1) Basic Information of Organization and Audit Requirement

Name of the Organisation	Centre for Excellence in Postal Technology Department of Posts Ministry of Communications Government of India.
Postal Address of the organisation	The General Manager Centre for Excellence in Postal Technology Bangalore Pincode:560001 Karnataka
Name of the contact person for Audit:	Shri. P S. Pavan Kumar (Deputy Director) CEPT, Mysuru Shri. C. Sri Nagesh (Assistant Director) CEPT, Hyderabad
Designation:	Deputy Director CEPT, Mysuru Assistant Director CEPT, Hyderabad
Telephone:	0821-2300999 040 - 23463645
Cell phone:	9449865958 (Deputy Director) CEPT, Mysuru 9490156728(Assistant Director) CEPT, Hyderabad
Email address:	ddcept.mysuru@indiapost.gov.in ad2cept.hyd@indiapost.gov.in
All machines:	
IP Addresses	Specific IP Addresses will be given after the Application Hosting in the NIC Meghraj Cloud Environment.
OS	Ubuntu 22.04
All machine names (DNS, WINS, Virtual Hosts, etc.)	Specific IP Addresses will be given after the Application Hosting in the NIC Meghraj Cloud Environment.
Is your organization subject to any specific regulatory requirements? (Examples – Sarbanes-Oxley, GLBA, HIPAA)	GIGW (Guidelines for Indian Government Websites) OWASP (Open Web Application Security Project)

Audit Information	
Would you like to perform a network-based assessment? (A&P)	Yes

How many Internet-facing hosts do you want to assess?	The application will be hosted in a NIC Meghraj cloud network and access will be provided to C-DAC for audit.
Would you like to perform a host-based assessment?	N/A
Which hosts?	N/A
Would you like to perform compliance, physical or enterprise assessment?	Compliance Assessment
If compliance, which regulations?	Yes, as per the GIGW (Guidelines for Indian Government Websites) OWASP (Open Web Application Security Project)
Would you like to perform an application security assessment?	Yes
Which specific applications? (URL, Application name, Installer, etc.)	DOP IT.2.0 https://test.cept.gov.in
Would you like this tested with or without administrative credentials?	With Administrative Credentials

2) Infrastructure

[DoP's applications will be hosted on the NIC Meghraj cloud. Details of the infrastructure will be shared with the bidders accordingly.]

3) Website and Web Applications

3.1) Web Application Name & URL

Details for Site 1	Mail Booking (Domestic, International, EMO) Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 2	Pick-up & Induction Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 3	Transmission Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 4	Delivery & Recruitment Solutions Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 5	PO Accounts Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 6	HR-1 Solutions Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 7	Internal Portals Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 8	Migration Solutions (Data Sanitization Solutions) Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 9	HR-2 Solutions Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 10	CRM Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 11	Customers Portals Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 12	IDAM, MDM & Integrations Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 13	PAO Accounts Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 14	IPS Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 15	Chat-Bot Solutions Live application URL will be provided after hosting the applications in the NIC Meghraj Cloud Servers

Details for Site 16	eFRM/Vigilance/Investigations Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.
Details for Site 17	BCP Management Solutions Live application URLs will be provided after hosting the applications in the NIC Meghraj Cloud Servers.

**3.2) Web Administrator:
Contact Person Name, Contact Number and Address**

Details for Site 1	Akbar Ali Khan Deputy Manager CEPT Mysuru Mobile: 8310373722 Email: akbar@indiapost.gov.in
Details for Site 2	Akbar Ali Khan Deputy Manager CEPT Mysuru Mobile: 8310373722 Email: akbar@indiapost.gov.in
Details for Site 3	ASNL. Rohini (Team Lead) CEPT Hyderabad Mobile: 9845824236 Email: rohini.asnl@indiapost.gov.in
Details for Site 4	Vinoth Kannan S (Team Lead) CEPT Mobile: 9786447723 Email: vinothkannan.s@indiapost.gov.in
Details for Site 5	Aravind Kumar (Team Lead) O/o CPMG, AP Circle Mobile: 9663451912 Email: v.aravind@indiapost.gov.in
Details for Site 6	Vijaya Lakshmi (Assistant Manager) CEPT Hyderabad Mobile: 9490425968 Email: vijaya.lakshmidivarakonda@indiapost.gov.in
Details for Site 7	Marra Chinnababu (Team Lead) CEPT Mobile: 8341781184 Email: chinna.m@indiapost.gov.in
Details for Site 8	Sreeroop. T (Team Lead) CEPT Kochi Mobile: 9995025671 Email: sreeroopt@gmail.com
Details for Site 9	Anil Raj (Team Lead) CEPT Mysuru Mobile: 9964556629 Email: anil.raj@indiapost.gov.in
Details for Site 10	G. Vidhyadhar (Team Lead) CEPT Hyderabad Mobile: 9052188318 Email: vidyadhar.guduru@indiapost.gov.in
Details for Site 11	Phani Kumar (Team Lead) CEPT Hyderabad Mobile: 9100249369 Email: chvs.phanikumar@indiapost.gov.in

Details for Site 12	Marra Chinnababu (Team Lead) CEPT Mobile: 8341781184 Email: chinna.m@indiapost.gov.in
Details for Site 13	V.Aravind Kumar (Team Lead) O/o CPMG, AP Circle Mobile: 9663451912 Email: v.aravind@indiapost.gov.in
Details for Site 14	Vinoth Kannan S (Team Lead) CEPT Mobile: 9786447723 Email: vinothkannan.s@indiapost.gov.in
Details for Site 15	Shreetej T. Ghodekar (Team Lead) CEPT Mumbai Mobile: 7303671362 Email: shreetej.ghodekar@indiapost.gov.in
Details for Site 16	G. Srikanth Dora (Team Lead) CEPT Mobile: 9040199780 Email: srikanta.dora@indiapost.gov.in
Details for Site 17	Revathi C.S (Team Lead) CEPT Mobile: 9884352152

3.3) Application/Website is accessible on Intranet or Internet

Details for Site 1	Internet
Details for Site 2	Internet
Details for Site 3	Internet
Details for Site 4	Internet
Details for Site 5	Internet
Details for Site 6	Internet
Details for Site 7	Internet
Details for Site 8	Internet
Details for Site 9	Internet
Details for Site 10	Internet
Details for Site 11	Internet
Details for Site 12	Internet
Details for Site 13	Internet
Details for Site 14	Internet
Details for Site 15	Internet
Details for Site 16	Internet
Details for Site 17	Internet

3.4) Brief about the website and activities done through the website

Details for Site 1	<ol style="list-style-type: none"> 1. Allows booking of Domestic, International & APS mail across Counters and accessible by Internal Users (Department Employees). 2. Allows all transactions for Retail products & services viz., Stamps sale, IPO Sale & Payment, ePost, eIPO, Bill Collections, Gangajal, Tiranga, Post Box/Bag fee, PO ID Card fee, etc across Counters and accessible by Internal Users (Department Employees). 3. Allows various transactions relating to Counters viz., Shift begin/end, reports, submit accounts, etc for the operators and supervisory options like counter allocation, authorization of transactions, verification of accounts etc. 4. Allows allocation of barcodes, and generation of various labels viz., address label, CN
---------------------------	---

	<p>22/23, Harmonized label, etc, including QR codes.</p> <p>5. Allows booking of Domestic Money Orders across Counters and accessible by Internal Users (Department Employees).</p>
Details for Site 2	<ol style="list-style-type: none"> 1. Induction of the articles based on the requests from web/mobile app/kiosk. 2. Handling Pickup requests. 3. Handling of the inventory in DoP. 4. Each 4x4 metre cell on a land parcel area of India will be given an identity i.e., Digital Address and is coded with a specific code called Digital Address Code.
Details for Site 3	<ol style="list-style-type: none"> 1. Handling, Transmission, Sorting and Aggregation of Mail between Booking and Delivery. 2. Master data mgmt of Sorting and Mail office Duty staff arrangements." 3. Booking, Despatch & Delivery of Logistic Post. 4. Creation of schedules, mapping of schedules to carriers, Onboarding of carriers, driver management, contract management, trip management & vehicle maintenance management. 5. Tracking Articles from Booking, in Transit and Delivery.
Details for Site 4	<ol style="list-style-type: none"> 1. This application is used for delivery the of Accountable articles and eMOs. 2. This application is used for receiving requests for the Return and Recall of the articles.
Details for Site 5	<ol style="list-style-type: none"> 1. Cash, Cheque, Stamps and Postal Stationery, IPOS management within the office between two offices, various MIS w.r.t. the same. 2. Generation of SO/ BO Summary, SO/ BO slips, ECB Memos, Transfer entries, Cashbook and Cash account, Closing and opening of BO bag and Account bags. 3. Cheque issue, cancel, reissue, Bank Scroll upload, Pairing of PO line items with Bank and various MIS w.r.t. the same. 4. Upload of files of focal point bank and RBI put through a statement at PAO level, Pairing of entries and related MIS.
Details for Site 6	<ol style="list-style-type: none"> 1. Creation and approval of new employee, adding family details, nomination, Communication details etc by employee. 2. Creation of Posts, modification, approval, view establishment register, upgrade, downgrade, redeploy, abolish etc and their approvals, post-to-post mapping. 3. option to apply different types of leaves through the self-service portal, their status view and view holiday calendar. 4. creating exit requests by employees and processing and generation of Retirement Benefits.
Details for Site 7	<ol style="list-style-type: none"> 1. Landing page containing the cards based on the roles of the user
Details for Site 8	<ol style="list-style-type: none"> 1. This website enables selected users to sanitize the identified master data available with DoP which will assist in the data migration activities.
Details for Site 9	<ol style="list-style-type: none"> 1. All Payroll related activities. 2. All Pay reimbursement, and Advances activities with approvals.
Details for Site 10	<ol style="list-style-type: none"> 1. Enabling customers to register with the Department of Posts and avail themselves of its online services. 2. Accept grievances through various channels such as the web portal, mobile app, email, chatbot, social media, and the PG portal. 3. Enables DOP employees to approve contracts and applications received from the bulk customers. 4. This application is designed for raising support desk tickets related to issues or problems encountered, as well as for seeking clarifications regarding applications, services, and network/hardware issues. It is intended for use by internal employees as well as vendors.
Details for Site 11	<ol style="list-style-type: none"> 1. "Enterprise Portal" is to serve as a one-stop destination for a diverse range of users, enabling them to access information and services offered by the Department of Posts through the Internet. This portal is designed to streamline operations and deliver services to the citizens' doorsteps, offering convenience, accessibility, and availability at any time and from anywhere. 2. To give Various Services to Philatelic Deposit account Holders and sale of stamps to the Public.

Details for Site 12	<p>1. Allows user creation, user authentication, access token generation, user enable/disable, event log maintenance, admin event log maintenance, and realm management.</p> <p>2. Allows module card creation, role creation, role modification, role mapping, user enable, user disable, and Single sign-on.</p> <p>3. Both Message and Mail Gateway solutions enable users to onboard applications to use the services provided by SMS and Email Service providers. Onboarding of Multiple Providers, SMS Template management, Provision of Dashboard, and required reports is also enabled.</p> <p>4. management of the Master data of Products, Offices, GL codes etc.</p> <p>5. Dynamic QR Payment method is implemented for integrating with other solutions</p>
Details for Site 13	<p>1. Budget allocation and related activities. Budget allocation, proposal upload, expenditure plan upload etc is done using Excel upload.</p> <p>2. PAO Modules deal with the account's consolidation from DDOs and further submission to PFMS and Pr AO Also create Transfer entries, objections management etc. HOA configurations and Management.</p>
Details for Site 14	1. Customs Clearance for Outbound International Articles
Details for Site 15	1. It is a chatbot that provides tracking of articles, tariffs of all mail products, location of the office, pin code of office, booking link, complaint status, complaint registration link, interest rates for saving schemes, answers banking faqs, provides details of postal insurance schemes.
Details for Site 16	1. The investigation application will deal with Fraud cases occurring at post offices. It will store all evidence related to a particular Fraud case. It will handle all the activities of fraud from preliminary case registration to till case close.
Details for Site 17	The application allows to manage and monitor the BCP period, activation, device utilization and dashboard across all offices per division in DoP.

3.5) Temporary URL / Staging Server URL

Details for Site 1	<p>Mail Booking (Domestic, International, EMO)</p> <p>Micro-service name URL Domestic & International Bookings---->https://test.cept.gov.in/mailbooking Retail and Third Party Bookings----->https://test.cept.gov.in/retailbooking Counter Operations-----> https://test.cept.gov.in/counterops Barcode Management----> https://test.cept.gov.in/labelmgmt/landing-page Money-Order Booking-----> https://test.cept.gov.in/mailbooking RFMS-----> https://test.cept.gov.in/retailbooking</p>
Details for Site 2	<p>Pick-up & Induction</p> <p>Micro-service name URL Induction Management-----> https://test.cept.gov.in/induction Pickup Management-----> https://test.cept.gov.in/pickup/dashboard Inventory Management-----> https://test.cept.gov.in/inventory Digital Address Code -----> https://dac.cept.gov.in</p>
Details for Site 3	<p>Transmission</p> <p>Micro-service name URL Bag Management-----> https://test.cept.gov.in/bagging Sorting Management-----> https://test.cept.gov.in/sorting Logistic Post-----> https://test.cept.gov.in/logisticpost Carrier &Schedule Management----->https://test.cept.gov.in/schedules Track & Trace-----> https://test.cept.gov.in/tracking</p>
Details for Site 4	<p>Delivery & Recruitment Solutions</p> <p>Micro-service name URL Postman & Delivery Management -----> https://test.cept.gov.in/delivery Recall & Return Management -----> https://test.cept.gov.in/delivery Recruitment solutions-----> yet to Develop front end(Url will be provided)</p>

Details for Site 5	PO Accounts Micro-service name URL Treasury Management-----> https://test.cept.gov.in/treasury Sub Accounts-----> https://test.cept.gov.in/subaccounts Bank Reconciliation(Po-level)-----> https://test.cept.gov.in/bankreconciliation Bank Reconciliation (PAO Level)-----> https://test.cept.gov.in/brspao
Details for Site 6	HR-1 Solutions Micro-service name URL PIS Module-----> https://test.cept.gov.in/pis Post Management-----> https://test.cept.gov.in/postmanagement Leave Management System-----> https://test.cept.gov.in/lms Exit Management-----> https://test.cept.gov.in/exitmgmt
Details for Site 7	Internal Portals URL -----> https://test.cept.gov.in/employeeportal
Details for Site 8	Migration Solutions (Data Sanitization Solutions) Micro-service name URL Data Sanitization Solutions-----> https://test.cept.gov.in/datasanitization
Details for Site 9	HR-2 Solutions Micro-service name URL Pay Roll (including Arrears) -----> https://dev.cept.gov.in/payroll/home Loans and Advances -----> https://dev.cept.gov.in/payroll/home
Details for Site 10	CRM Micro-service name URL Portal for External Customers-----> https://test.cept.gov.in/crm Grievance Management-----> https://test.cept.gov.in/grievances Customer Management-----> https://test.cept.gov.in/internalcrm Support Desk Management System-----> https://test.cept.gov.in/supportdesk
Details for Site 11	Customers Portals Micro-service name URL Enterprise Portal-----> https://test.cept.gov.in/enterpriseportal/home Philately Stamps Portal -----> https://test.cept.gov.in/philately/home
Details for Site 12	IDAM, MDM & Integrations Micro-service name URL IDAM-----> https://test.cept.gov.in/idam/admin/master/console Role Management-----> https://test.cept.gov.in/itrolemgmt/home Message Gateway-----> https://test.cept.gov.in/bemsggateway/ Mail Gateway-----> http://test.cept.gov.in/bemailgateway Master Data Management(MDM)---> yet to Develop front end(Url will be provided) Payment Gateway -----> yet to Develop front end (URL will be provided)
Details for Site 13	PAO Accounts Micro-service name URL (Budget) -----> https://test.cept.gov.in/budget (PAO Module)-----> https://test.cept.gov.in/pao
Details for Site 14	IPS Micro-service name URL New IPS & DNK Middle Layer -----> https://test.cept.gov.in/ips
Details for Site 15	Chat-Bot Solutions URL: ----- https://test.cept.gov.in/bechatbot/webhooks/custom/webhook

Details for Site 16	eFRM/Vigilance/Investigations investigation -----> https://dev.cept.gov.in/investigation
Details for Site 17	BCP Management Solutions BCP -----> https://dev.cept.gov.in/bcpsolution

3.6) Number of Roles in the Application

Details for Site 1	Domestic & International Bookings: 2 Roles. Retail and Third-Party Bookings: 4 Roles. Counter Operations: 2 Roles. Barcode Management: 4 Roles. Money-Order Booking: 4 Roles. RFMS: 3 Roles.
Details for Site 2	Induction Management: 2 Roles Pickup Management: 2 Roles Inventory Management: 2Roles Digital Address code: 1 Role
Details for Site 3	Bagging: 10 roles. Sorting: 19 roles. LogisticPost: 2 roles. Schedules: 6 roles. Tracking: 01 role.
Details for Site 4	Postman & Delivery Management: 2 Roles. Recall & Return Management: 1 Role.
Details for Site 5	Treasury: 4 roles. Sub-Accounts: 3 roles. Bank reconciliation: 2 roles.
Details for Site 6	Pis: 5 roles; Post management: 2 roles; LMS: 3 roles; Exit management: 6 roles.
Details for Site 7	1 Role
Details for Site 8	3 Roles, with Read, Write and Update privileges.
Details for Site 9	Pay Roll (including Arrears): 4 Roles. Loans and Advances: 4 Roles.
Details for Site 10	Portal for External Customers: 1 Role Grievance Management: 2 Roles. Customer Management: 6 Roles Support Desk Management System: 4 Roles.
Details for Site 11	Enterprise Portal: 4 Roles. Philately Stamps Portal: 4 Roles.
Details for Site 12	IDAM: 1 Role Role Management: 2 Roles. Message & Mail Gateway: 4 Roles. Master Data Management (MDM): 4 Roles. Payment Gateway Solutions: 2 Roles.
Details for Site 13	Budget: 6 Roles. PAO Module: 7 Roles.
Details for Site 14	7 Roles
Details for Site 15	0 Roles.
Details for Site 16	3 Roles.
Details for Site 17	

3.7) Number of static pages

Details for Site 1	0
---------------------------	---

Details for Site 2	0
Details for Site 3	0
Details for Site 4	0
Details for Site 5	0
Details for Site 6	0
Details for Site 7	0
Details for Site 8	2
Details for Site 9	0
Details for Site 10	20
Details for Site 11	171
Details for Site 12	4
Details for Site 13	68
Details for Site 14	0
Details for Site 15	0
Details for Site 16	0
Details for Site 17	

3.8) Number of Dynamic Pages

Details for Site 1	71
Details for Site 2	33
Details for Site 3	109
Details for Site 4	1
Details for Site 5	53
Details for Site 6	109
Details for Site 7	1
Details for Site 8	22
Details for Site 9	39
Details for Site 10	122
Details for Site 11	131
Details for Site 12	138
Details for Site 13	64
Details for Site 14	10
Details for Site 15	0
Details for Site 16	75
Details for Site 17	

3.9) Number of User Input fields (approximately)

Details for Site 1	834
Details for Site 2	108
Details for Site 3	770
Details for Site 4	13
Details for Site 5	242
Details for Site 6	366
Details for Site 7	0
Details for Site 8	800
Details for Site 9	140
Details for Site 10	597
Details for Site 11	150
Details for Site 12	866
Details for Site 13	70
Details for Site 14	20
Details for Site 15	0
Details for Site 16	240
Details for Site 17	

3.10) Operating System details with version

Details for Site 1	Ubuntu 22.04 LTS
Details for Site 2	Ubuntu 22.04.4 LTS
Details for Site 3	Ubuntu 22.04.4 LTS
Details for Site 4	Ubuntu 22.04.4 LTS
Details for Site 5	Ubuntu 22.04.4 LTS
Details for Site 6	Ubuntu 22.04.4 LTS
Details for Site 7	Ubuntu 22.04.4 LTS
Details for Site 8	Ubuntu 22.04.4 LTS
Details for Site 9	Ubuntu 22.04.4 LTS
Details for Site 10	Ubuntu 22.04.4 LTS
Details for Site 11	Ubuntu 22.04.4 LTS
Details for Site 12	Ubuntu 22.04.4 LTS
Details for Site 13	Ubuntu 22.04.4 LTS
Details for Site 14	Ubuntu 22.04.4 LTS
Details for Site 15	Ubuntu 22.04.4 LTS
Details for Site 16	Ubuntu 22.04.4 LTS
Details for Site 17	

3.11) Web server details with version

Details for Site 1	Apache, Nginx
Details for Site 2	Apache, Nginx
Details for Site 3	Apache, Nginx
Details for Site 4	Apache, Nginx
Details for Site 5	Apache, Nginx
Details for Site 6	Apache, Nginx
Details for Site 7	Apache, Nginx
Details for Site 8	Apache, Nginx
Details for Site 9	Apache, Nginx
Details for Site 10	Apache, Nginx
Details for Site 11	Apache, Nginx
Details for Site 12	Apache, Nginx
Details for Site 13	Apache, Nginx
Details for Site 14	Apache, Nginx
Details for Site 15	Apache, Nginx
Details for Site 16	Apache, Nginx
Details for Site 17	

3.12) Back-end database with version

Details for Site 1	Postgres Version:16
Details for Site 2	Postgres Version:16
Details for Site 3	Postgres Version:16
Details for Site 4	Postgres Version:16
Details for Site 5	Postgres Version:16
Details for Site 6	Postgres Version:16
Details for Site 7	Postgres Version:16
Details for Site 8	Postgres Version:16
Details for Site 9	Postgres Version:16
Details for Site 10	Postgres Version:16
Details for Site 11	Postgres Version:16
Details for Site 12	Postgres Version:16
Details for Site 13	Postgres Version:16
Details for Site 14	Postgres Version:16
Details for Site 15	Postgres Version:16

Details for Site 16	Postgres Version:16
Details for Site 17	

3.13) Front-end tools/Server-Side Scripts/Programming tools used with version details

Details for Site 1	ReactJS, NextJS, Golang,
Details for Site 2	ReactJS, NextJS, Golang, Leaflet
Details for Site 3	ReactJS, NextJS, Golang,
Details for Site 4	ReactJS, NextJS, Golang,
Details for Site 5	ReactJS, NextJS, Golang,
Details for Site 6	ReactJS, NextJS, Golang,
Details for Site 7	ReactJS, NextJS, Golang,
Details for Site 8	ReactJS, NextJS, Golang,
Details for Site 9	ReactJS, NextJS, Golang,
Details for Site 10	ReactJS, NextJS, Golang,
Details for Site 11	ReactJS, NextJS, Golang,
Details for Site 12	ReactJS, NextJS, Golang, Java
Details for Site 13	ReactJS, NextJS, Golang,
Details for Site 14	ReactJS, NextJS, Golang,
Details for Site 15	Python.
Details for Site 16	ReactJS, NextJS, Golang,
Details for Site 17	ReactJS, NextJS, Golang,

3.14) Document/report details HTML, PDF, XML etc

Details for Site 1	HTML
Details for Site 2	HTML
Details for Site 3	HTML
Details for Site 4	HTML
Details for Site 5	HTML
Details for Site 6	HTML
Details for Site 7	HTML
Details for Site 8	HTML
Details for Site 9	HTML
Details for Site 10	HTML
Details for Site 11	HTML
Details for Site 12	HTML
Details for Site 13	HTML
Details for Site 14	HTML
Details for Site 15	HTML
Details for Site 16	HTML
Details for Site 17	

3.15) Any coding frameworks used (Eg: Codeigniter, Laravel, Silverlight etc)

Details for Site 1	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 2	Golang Template Customised, React Template Customised Next JS Template Customised, Leaflet
Details for Site 3	React, Next Js, Golang gin, Squirrel
Details for Site 4	Golang Template Customised, React Template Customised Next JS Template Customised

Details for Site 5	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 6	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 7	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 8	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 9	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 10	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 11	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 12	Keycloak customised, Golang Template Customised, React Template Customised Next JS Template Customised.
Details for Site 13	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 14	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 15	RASA
Details for Site 16	Golang Template Customised, React Template Customised Next JS Template Customised
Details for Site 17	

3.16) Total number of input forms

Details for Site 1	56
Details for Site 2	11
Details for Site 3	98
Details for Site 4	1
Details for Site 5	53
Details for Site 6	37
Details for Site 7	0
Details for Site 8	75
Details for Site 9	39
Details for Site 10	62
Details for Site 11	60
Details for Site 12	133
Details for Site 13	34
Details for Site 14	5
Details for Site 15	0
Details for Site 16	55
Details for Site 17	

3.17) Type of Webservice (Restful, SOAP etc)

Details for Site 1	Restful- JSON
Details for Site 2	Restful- JSON
Details for Site 3	Restful- JSON
Details for Site 4	Restful- JSON
Details for Site 5	Restful- JSON
Details for Site 6	Restful- JSON
Details for Site 7	Restful- JSON
Details for Site 8	Restful- JSON
Details for Site 9	Restful- JSON
Details for Site 10	Restful- JSON
Details for Site 11	Restful- JSON
Details for Site 12	Restful- JSON
Details for Site 13	Restful- JSON
Details for Site 14	Restful- JSON
Details for Site 15	Restful- JSON
Details for Site 16	Restful- JSON
Details for Site 17	Restful- JSON

3.18) Payment Gateway integrated with the application YES/NO

Details for Site 1	Yes
Details for Site 2	Yes
Details for Site 3	No
Details for Site 4	Yes
Details for Site 5	No
Details for Site 6	No
Details for Site 7	No
Details for Site 8	No
Details for Site 9	No
Details for Site 10	Yes
Details for Site 11	Yes
Details for Site 12	No
Details for Site 13	No
Details for Site 14	No
Details for Site 15	No
Details for Site 16	No
Details for Site 17	No

3.19) Number of Methods / Parameters

Details for Site 1	183
Details for Site 2	244
Details for Site 3	254
Details for Site 4	111
Details for Site 5	110
Details for Site 6	1474
Details for Site 7	1
Details for Site 8	320
Details for Site 9	94
Details for Site 10	66
Details for Site 11	434
Details for Site 12	968
Details for Site 13	81
Details for Site 14	30
Details for Site 15	22

Details for Site 16	63
Details for Site 17	10

3.20) Location of the work (Onsite (Internal) or offsite (external))

Details for Site 1	Onsite/Internal
Details for Site 2	Onsite/Internal
Details for Site 3	Onsite/Internal
Details for Site 4	Onsite/Internal
Details for Site 5	Onsite/Internal
Details for Site 6	Onsite/Internal
Details for Site 7	Onsite/Internal
Details for Site 8	Onsite/Internal
Details for Site 9	Onsite/Internal
Details for Site 10	Onsite/Internal/External
Details for Site 11	Onsite/Internal
Details for Site 12	Onsite/Internal
Details for Site 13	Onsite/Internal
Details for Site 14	Onsite/Internal
Details for Site 15	Onsite/Internal
Details for Site 16	Onsite/Internal
Details for Site 17	

3.21) Are any other specific technologies or 3rd party components used?

Details for Site 1	Minio
Details for Site 2	Leaflet
Details for Site 3	No
Details for Site 4	0
Details for Site 5	No
Details for Site 6	No
Details for Site 7	No
Details for Site 8	2FA (2 Factor Authentication)
Details for Site 9	No
Details for Site 10	Min io
Details for Site 11	Yes (Bhashini has been integrated for multilingual support)
Details for Site 12	APIs provided by CDAC and NIC are used. A relay SMTP server is used for sending mail
Details for Site 13	No
Details for Site 14	No
Details for Site 15	No
Details for Site 16	No
Details for Site 17	Chart js

3.22) Whether the web application contains any Content Management System. If yes, please mention the name of the CMS.

Details for Site 1	No
Details for Site 2	No
Details for Site 3	No
Details for Site 4	No

Details for Site 5	No
Details for Site 6	No
Details for Site 7	No
Details for Site 8	No
Details for Site 9	No
Details for Site 10	No
Details for Site 11	Yes
Details for Site 12	No
Details for Site 13	No
Details for Site 14	No
Details for Site 15	No
Details for Site 16	No
Details for Site 17	

3.23) Please share sample login credentials, one for each role Yes/No.

3.24) Please share SRS or technical documents of the website if any are available Yes/No.

Details for Site 1	Yes
Details for Site 2	Yes
Details for Site 3	Yes
Details for Site 4	Yes
Details for Site 5	Yes
Details for Site 6	Yes
Details for Site 7	Yes
Details for Site 8	Yes
Details for Site 9	Yes
Details for Site 10	Yes
Details for Site 11	Yes
Details for Site 12	Yes
Details for Site 13	Yes
Details for Site 14	Yes
Details for Site 15	
Details for Site 16	
Details for Site 17	

3.25) Will the website/web application/web service be available remotely for auditing (Yes/No)

(If No, then the auditors will have to travel to client premises and the costs shall include the travel and accommodation charges)

Details for Site 1	Minio S3
Details for Site 2	Minio S3
Details for Site 3	Minio S3
Details for Site 4	Minio S3
Details for Site 5	Minio S3
Details for Site 6	Minio S3
Details for Site 7	Minio S3
Details for Site 8	Minio S3
Details for Site 9	Minio S3
Details for Site 10	Minio S3
Details for Site 11	Minio S3
Details for Site 12	Minio S3
Details for Site 13	Minio S3

Details for Site 14	Minio S3
Details for Site 15	Minio S3
Details for Site 16	Minio S3
Details for Site 17	

3.26) Are you maintaining Application Logs?

Details for Site 1	Yes
Details for Site 2	Yes
Details for Site 3	Yes
Details for Site 4	Yes
Details for Site 5	Yes
Details for Site 6	Yes
Details for Site 7	Yes
Details for Site 8	Yes
Details for Site 9	Yes
Details for Site 10	Yes
Details for Site 11	Yes
Details for Site 12	Yes
Details for Site 13	Yes
Details for Site 14	Yes
Details for Site 15	No
Details for Site 16	No
Details for Site 17	

3.27) Willing to provide server remote connection to collect the log evidence (Yes/No)

To get OWASP Top 10 2017 Compliance, this is mandatory. If you answer No to this, then we will not be able to provide the OWASP 2017 complaint certificate.

Details for Site 1	Yes
Details for Site 2	Yes
Details for Site 3	Yes
Details for Site 4	Yes
Details for Site 5	Yes
Details for Site 6	Yes
Details for Site 7	Yes
Details for Site 8	Yes
Details for Site 9	Yes
Details for Site 10	Yes
Details for Site 11	Yes
Details for Site 12	Yes
Details for Site 13	Yes
Details for Site 14	Yes
Details for Site 15	Yes
Details for Site 16	Yes
Details for Site 17	

3.28) Please share previous audit reports if any are done or available (Yes/No).

4) Mobile Application

Details of the Mobile Applications					
Sl. No	Head		Details for Mobile Application 1	Details for Mobile Application 2	Details for Mobile application 3
1	Name of the Mobile application		DOP Internal Mobile App	DOP ESS 2.0 APP	IndiaPost APP
2	Web Administrator: Contact Person Name, Contact Number and Address		Vinayak S Shetti ASP CEPT Mysuru-570010 Email: vinayaks@indiapost.gov.in Mobile: 9449849337	Vinayak S Shetti ASP CEPT Mysuru-570010 Email: vinayaks@indiapost.gov.in Mobile: 9449849337	Phani Kumar (Team Lead) CEPT Hyderabad Mobile: 9100249369 Email: chvs.phanikumar@indiapost.gov.in
3	Type of Application, Native or Hybrid		Hybrid	Hybrid	Hybrid
4	Supportive Operating System	Android	Android	Android	Android
5	Does the application have a login interface if so, how many user roles are available?		Yes, 3 Roles	3 Roles	Yes,7 Roles
6	Brief about the mobile application and activities done through the mobile application		DOP Internal Mobile App: Postal Operations by the employees ESS 2.0 APP: Employee self-service like leave, reimbursements etc	DOP Internal Mobile App: Postal Operations by the employees ESS 2.0 APP: Employee self-service like leave, reimbursements etc	DOP Customer Mobile APP: Postal services used by the Outside customers. Postal services like Article Booking, MO booking, Pickup requests, Locate Post Offices, Track N Trace, User Registration, Contract creation, Raising complaints and information on postal services etc

7	Number of Screens		73	23	158
8	Number of Activities		82	17	44
9	Number of User Input fields (approximately)		228	111	223
10	Is there any web service which the app interacts with, if so, do you want the web service also to be audited	YES, Interacted with GO API	YES, Interacted with GO API	YES, Interacted with GO API	YES, Interacted with GO API
11	Payment Gateway Integrated with the application (YES / No)		Yes	Yes	Yes
12	Please share the Mobile application User manual or SRS	ATTACHED			
13	Please share previous audit reports if any are done or available Yes/No.	YES	YES	YES	YES

Annexure 7 – MeitY Guidelines on Cybersecurity Audit

1. Comprehensive audit

1.1. Comprehensive audit should be done at least once in a year and should cover the entire application, including the following:

- a) web application (both thick client and thin client);
- b) mobile apps.
- c) APIs (including API whitelisting);
- d) databases.
- e) Hosting infrastructure and obsolescence.
- f) Cloud hosting platform and network infrastructure; and
- g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and the Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant information security best practice, including, in particular, use of Aadhaar Data vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

1.2. The scope of the comprehensive audit should include, inter alia, the following:

- a) Source code assessment.
- b) Application security assessment (both Black Box and Grey Box testing), including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application Design, Implementation and Analysis.
- c) network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end-of-life/support particulars; whether a centralized platform exists for pushing patch updates and antivirus and whether there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs);
- d) penetration testing;
- e) network and device configuration review;
- f) application hosting configuration review;
- g) database security assessment (including whether personal data is being encrypted at rest and in motion, used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication);
- h) user access controls (including privilege access management) and access reconciliation review;

- i) identity and access management controls review;
 - j) data protection controls review (inter alia, regarding advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks ICIAD-2021-0004");
 - k) security operations and monitoring review (including maintenance of security logs, correlation and analysis);
 - l) review of logs, backup and archival data for access to personal data (including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in the exercise of powers vested in it by law); and
 - m) review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website).
- 1.3. The auditor should be CERT-In-empaneled and, in case of application hosted on cloud, the auditor should have the capability for carrying out cloud security audit as per the empanelment details available on CERT-In's website.

2. Limited audit

- 2.1. Limited audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is-
- (a) modification in application functionality; or
 - (b) addition/modification of APIs; or
 - (c) migration to new infrastructure platform or cloud service; or
 - (d) change in configuration of application hosting, servers, network components and security devices; or
 - (e) change in access control policy.
- 2.2. The scope of limited audit should include, inter alia, the following:
- (a) In all cases: Source code assessment; application security assessment (both Black Box and Grey Box testing) including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;
 - (b) In case limited audit is after six months of comprehensive audit: In addition to (a) above, user access controls (including privilege access management) and access reconciliation review; identity and access management controls review.
 - (c) In case limited audit is done earlier: In addition to (a) and (b) above,-
 - (i) For audit on modification in application functionality, addition/modification of APIs, migration to new infrastructure platform or cloud service or change in configuration of application hosting, servers, network components and security devices: Network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of Life /support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs); network and device configuration review; application hosting configuration review; database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multifactor authentication); data protection controls review (inter alia, with

reference to advisories issued by CERT-IN from time to time regarding prevention of data leaks, including "preventing Data Breaches / Data Leaks [CIAD-202 I -0004]"); security operations and monitoring review (including maintenance of security logs, review of logs, integration with security monitoring solution, correlation and analysis; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); review of logs, backup and archival data specifically for access to personal data; review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in ' the Aadhaar Authentication Application Security Standard available on UIDAI's website); and

(ii) For audit on change in access control policy; Review of logs and integration with security monitoring solutions.

Annexure 8 – Transaction Definition

In the context of DoP, a transaction would represent the end-to-end process of service delivery or information exchange within a specific vertical of DoP, impacting its respective applications. It may refer to any individual or group of actions or exchanges that involve the transfer, processing, or exchange of information, goods, or services between the DoP and its customers, partners, or internal systems, executed through one of its vertical-specific applications. Each transaction is typically completed through a defined workflow within the application and would result in a measurable outcome such as a financial update, status change, or record modification.

For example:

1. Banking

The Department of Posts offers a range of financial services under its **Post Office Savings Bank (POSB)** system, which functions like a regular bank.

i. Example of a transaction: Account Deposit or Withdrawal

A customer visits the post office or uses an online banking portal to deposit or withdraw funds from their savings account. This transaction involves updating the customer's account balance in the system, generating a receipt or confirmation, and potentially notifying the customer via SMS or email. The application records the deposit or withdrawal in real time, updating the financial records.

ii. Example of a transaction: Fund Transfer

A customer initiates a fund transfer from their Post Office savings account to another bank account. This involves checking the balance, validating account details, transferring the specified amount, and confirming the transaction. The application may also interact with the payment gateway for real-time fund transfers.

2. Insurance

The Department of Posts provides insurance services through the **Postal Life Insurance (PLI)** and **Rural Postal Life Insurance (RPLI)** schemes.

i. Example of a transaction: Policy Issuance

A customer applies for a life insurance policy via the Post Office. This transaction involves the collection of customer details, the calculation of premium rates based on risk factors, policy issuance, and the generation of an insurance certificate. The insurance application processes the data and updates the customer's profile with the new policy details.

ii. Example of a transaction: Premium Payment

A policyholder makes a premium payment, either in person or online. The system processes the payment, updates the policy status, and generates a payment receipt. This transaction includes updating the insurance ledger and ensuring the policy remains active.

iii. Example of a transaction: Claim Processing

A claim is submitted by the beneficiary or policyholder. The insurance application tracks the claim, validates the details, and initiates the process of settlement or rejection. The transaction involves various steps such as verification of documents, calculation of claim amount, and payment disbursement.

3. Postal Operations

The core of the Department of Posts involves the delivery and receipt of letters, parcels, and other physical mail services.

i. **Example of a transaction: Parcel Booking**

A customer books a parcel to be delivered to a specific location. This transaction includes recording the sender and recipient's details, calculating postage fees, accepting payment, and generating a tracking number. The system then updates the logistics records as the parcel moves through different stages of delivery.

ii. **Example of a transaction: Parcel or Letter Delivery**

Once the parcel reaches its destination, the system updates the status to "delivered," logs the time of delivery, and may capture electronic proof of delivery (e.g., signature or photo confirmation). The application ensures all delivery checkpoints are captured and logged in real-time for the sender to track.

4. Mail Operations

Mail operations cover the logistics, sorting, and routing of postal mail, ensuring the smooth movement of letters and packages across locations.

i. **Example of a transaction: Sorting and Dispatch**

As mail arrives at a central sorting facility, the application tracks each item's journey as it is sorted and routed to the appropriate delivery centre. This transaction involves scanning, assigning, and updating the mail's status as it progresses from one step to another. The system must ensure accurate routing, and each update is tracked for efficiency and accuracy.

ii. **Example of a transaction: Delivery Confirmation for Registered Mail**

Registered mail requires proof of delivery. When a registered letter or parcel is delivered, the transaction captures the recipient's signature electronically, updates the system, and notifies the sender that the delivery has been completed. This data is logged within the mail operations application for traceability.

5. Business Development Services

This vertical involves services such as **e-commerce logistics**, partnerships with businesses, and new product development for corporate clients.

i. **Example of a transaction: E-commerce Delivery Service**

A business partner (e.g., an e-commerce company) utilizes the Department of Posts for logistics and delivery. When a business submits an order to the Post, the application processes it, assigns it to a delivery route, and tracks the package's journey from the warehouse to the customer. Each movement of the parcel—from pickup, transit, to delivery—is tracked, and status updates are shared with the e-commerce business.

ii. **Example of a transaction: New Client Onboarding**

A new corporate client seeks to engage the Post for business services (e.g., bulk

mail delivery or warehousing). The transaction involves setting up the client in the system, defining service levels, setting up payment terms, and signing the contract. Once the setup is complete, future transactions such as bulk deliveries or special services are logged under the client's account.

Annexure 9 – Eligibility Criteria

S.No	Eligibility Criteria	Supporting Required
1	Bidder must be a Government Organization / PSU / PSE / partnership firm / LLP or private / public limited company in India at least for the last 5 years	Documentary Proof to be attached (Certificate of Incorporation)
2	Bidder must not be blacklisted / debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs) as on the date of proposal submission	Letter of confirmation from Bidder.
3	The Bidder must have registered a turnover of Rs. 10 Crores or above (from Indian Operations only) in each year during the last three completed financial years–2021-22, 2022- 23 & 2023-24 (Not inclusive of the turnover of associate companies)	Audited Financial statements for the financial years 2021-22, 2022- 23 & 2023-24 Certified letter from the Chartered Accountant.
4	The Bidder must be Net profit making entity (from Indian operations only) continuously for the last three years that is financial years – 2021-22, 2022- 23 & 2023-24	Audited Financial statements for the financial years 2021-22, 2022- 23 & 2023-24 Certified letter from the Chartered Accountant.
5	The Bidder should be empanelled by CERT- In as on the last date of submission of proposal. It is the responsibility of the successful vendor to submit renewed certificate in case Cert-IN empanelment validity expiring during the contract period, failing which DoP will terminate the contract.	Documentary Proof to be attached
6	Bidder shall provide a signed copy of the Integrity pact	Signed Integrity pact as per format



Bid Number/बोली क्रमांक (बिड संख्या):
GEM/2024/B/5672506
Dated/दिनांक : 06-12-2024

Bid Document/ बिड दस्तावेज़

Bid Details/बिड विवरण	
Bid End Date/Time/बिड बंद होने की तारीख/समय	27-12-2024 20:00:00
Bid Opening Date/Time/बिड खुलने की तारीख/समय	27-12-2024 20:30:00
Bid Offer Validity (From End Date)/बिड पेशकश वैधता (बंद होने की तारीख से)	30 (Days)
Ministry/State Name/मंत्रालय/राज्य का नाम	Ministry Of Communications
Department Name/विभाग का नाम	Department Of Posts
Organisation Name/संगठन का नाम	Department Of Posts
Office Name/कार्यालय का नाम	Postal Directorate, Dak Bhawan, New Delhi
Item Category/मद केटेगरी	Custom Bid for Services - RFP For Information Security Audit and Performance Testing
Similar Category/समान श्रेणी	<ul style="list-style-type: none">• Cyber Security Audit• Vulnerability and Penetration Testing• Financial Audit Services
Contract Period/अनुबंध अवधि	5 Year(s)
Minimum Average Annual Turnover of the bidder (For 3 Years)/बिडर का न्यूनतम औसत वार्षिक टर्नओवर (3 वर्षों का)	1000 Lakh (s)
MSE Exemption for Years of Experience and Turnover/ अनुभव के वर्षों से एमएसई छूट	No
Startup Exemption for Years of Experience and Turnover/ अनुभव के वर्षों से स्टार्टअप छूट	No
Document required from seller/विक्रेता से मांगे गए दस्तावेज़	Experience Criteria,Bidder Turnover,Certificate (Requested in ATC),Additional Doc 1 (Requested in ATC) *In case any bidder is seeking exemption from Experience / Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer
Do you want to show documents uploaded by bidders to all bidders participated in bid?/	Yes
Bid to RA enabled/बिड से रिवर्स नीलामी सक्रिय किया	No
Type of Bid/बिड का प्रकार	Two Packet Bid

Bid Details/बिड विवरण

Time allowed for Technical Clarifications during technical evaluation/तकनीकी मूल्यांकन के दौरान तकनीकी स्पष्टीकरण हेतु अनुमत समय	2 Days
Estimated Bid Value/अनुमानित बिड मूल्य	348100000
Evaluation Method/मूल्यांकन पद्धति	Total value wise evaluation
Financial Document Indicating Price Breakup Required/मूल्य दर्शाने वाला वित्तीय दस्तावेज ब्रेकअप आवश्यक है	Yes
Arbitration Clause	No
Mediation Clause	No

EMD Detail/ईएमडी विवरण

Advisory Bank/एडवाइजरी बैंक	State Bank of India
EMD Amount/ईएमडी राशि	6000000

ePBG Detail/ईपीबीजी विवरण

Advisory Bank/एडवाइजरी बैंक	State Bank of India
ePBG Percentage(%) /ईपीबीजी प्रतिशत (%)	5.00
Duration of ePBG required (Months)/ईपीबीजी की अपेक्षित अवधि (महीने).	62

(a). EMD EXEMPTION: The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. Traders are excluded from the purview of this Policy./जेम की शर्तों के अनुसार ईएमडी छूट के इच्छुक बिडर को संबंधित केटेगरी के लिए बिड के साथ वैध समर्थित दस्तावेज प्रस्तुत करने हैं। एमएसई केटेगरी के अंतर्गत केवल वस्तुओं के लिए विनिर्माता तथा सेवाओं के लिए सेवा प्रदाता ईएमडी से छूट के पात्र हैं। व्यापारियों को इस नीति के दायरे से बाहर रखा गया है।

(b). EMD & Performance security should be in favour of Beneficiary, wherever it is applicable./ईएमडी और संपादन जमानत राशि, जहां यह लागू होती है, लाभार्थी के पक्ष में होनी चाहिए।

Beneficiary/लाभार्थी :

ADG PMU
Postal Directorate, Dak Bhawan, New Delhi, Department of Posts, Department of Posts, Ministry of Communications
(Adg Pmu)

MII Compliance/एमआईआई अनुपालन

MII Compliance/एमआईआई अनुपालन	Yes
-------------------------------	-----

MSE Purchase Preference/एमएसई खरीद वरीयता

MSE Purchase Preference/एमएसई खरीद वरीयता	Yes
---	-----

1. The minimum average annual financial turnover of the bidder during the last three years, ending on 31st March of the previous financial year, should be as indicated above in the bid document. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution / incorporation of the bidder is less than 3-year-old, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criteria.

2. Purchase preference to Micro and Small Enterprises (MSEs): Purchase preference will be given to MSEs as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. If the bidder wants to avail the Purchase preference for services, the bidder must be the Service provider of the offered Service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered service. If L-1 is not an MSE and MSE Service Provider (s) has/have quoted price within L-1+ 15% of margin of purchase preference /price band as defined in the relevant policy, then 100% order quantity will be awarded to such MSE bidder subject to acceptance of L1 bid price. The buyers are advised to refer to the [OM No.1 4 2021 PPD dated 18.05.2023](#) for compliance of Concurrent application of Public Procurement Policy for Micro and Small Enterprises Order, 2012 and Public Procurement (Preference to Make in India) Order, 2017. Benefits of MSE will be allowed only if the credentials of the service provider are validated on-line in GeM profile as well as validated and approved by the Buyer after evaluation of submitted documents.

3. If L-1 is not an MSE and MSE Service Provider (s) has/have quoted price within L-1+ 15% of margin of purchase preference /price band as defined in the relevant policy, then 100% order quantity will be awarded to such MSE bidder subject to acceptance of L1 bid price.

4. Estimated Bid Value indicated above is being declared solely for the purpose of guidance on EMD amount and for determining the Eligibility Criteria related to Turn Over, Past Performance and Project / Past Experience etc. This has no relevance or bearing on the price to be quoted by the bidders and is also not going to have any impact on bid participation. Also this is not going to be used as a criteria in determining reasonableness of quoted prices which would be determined by the buyer based on its own assessment of reasonableness and based on competitive prices received in Bid / RA process.

Additional Qualification/Data Required/अतिरिक्त योग्यता /आवश्यक डेटा

Scope of Work:[1733491448.pdf](#)

Payment Terms:[1733491459.pdf](#)

GEM Availability Report (GAR):[1733491498.pdf](#)

Undertaking of Competent Authority is mandatory to create Custom Bid for Services. Please download standard format document and upload:[1733491516.pdf](#)

This Bid is based on Least Cost Method Based Evaluation (LCS). The technical qualification parameters are:-

Parameter Name	Max Marks	Min Marks	Evaluation Document	Seller Document Required
As per details mentioned in the RFP document	100	70	View file	Yes

Total Minimum Passing Technical Marks: 70

Pre Bid Detail(s)

Pre-Bid Date and Time	Pre-Bid Venue
07-12-2024 18:00:00	Meeting link ID: 7571490712 Password: 684860 Join Meeting https://bharatvc.nic.in/join/7571490712

Custom Bid For Services - RFP For Information Security Audit And Performance Testing (1)

Technical Specifications/तकनीकी विशिष्टियाँ

Specification	Values
Core	
Description /Nomenclature of Service Proposed for procurement using custom bid functionality	RFP For Information Security Audit and Performance Testing
Regulatory/ Statutory Compliance of Service	YES
Compliance of Service to SOW, STC, SLA etc	YES
Addon(s)/एडऑन	

Additional Specification Documents/अतिरिक्त विशिष्टि दस्तावेज़

Consignees/Reporting Officer/परेषिती/रिपोर्टिंग अधिकारी

S.No./क्र. सं.	Consignee Reporting/Officer/ परेषिती/रिपोर्टिंग अधिकारी	Address/पता	The quantity of procurement "1" indicates Project based or Lumpsum based hiring.	Additional Requirement/अतिरिक्त आवश्यकता
1	Rituraj Yadav	110001,Room No. 411 & 422, Dak Bhawan, Sansad Marg New Delhi- 110001	1	N/A

Buyer Added Bid Specific Terms and Conditions/क्रेता द्वारा जोड़ी गई बिड की विशेष शर्तें

1. Generic

OPTION CLAUSE: The buyer can increase or decrease the contract quantity or contract duration up to 25 percent at the time of issue of the contract. However, once the contract is issued, contract quantity or contract duration can only be increased up to 25 percent. Bidders are bound to accept the revised quantity or duration

2. Buyer Added Bid Specific ATC

Buyer uploaded ATC document [Click here to view the file.](#)

3. Buyer Added Bid Specific ATC

Buyer Added text based ATC clauses

Pre bid meeting link

Meeting link ID:

7571490712

Password:

684860

Join Meeting

<https://bharatvc.nic.in/join/7571490712>

Disclaimer/अस्वीकरण

The additional terms and conditions have been incorporated by the Buyer after approval of the Competent Authority in Buyer Organization, whereby Buyer organization is solely responsible for the impact of these clauses on the bidding process, its outcome, and consequences thereof including any eccentricity / restriction arising in the bidding process due to these ATCs and due to modification of technical specifications and / or terms and conditions governing the bid. If any clause(s) is / are incorporated by the Buyer regarding following, the bid and resultant contracts shall be treated as null and void and such bids may be cancelled by GeM at any stage of bidding process without any notice:-

1. Definition of Class I and Class II suppliers in the bid not in line with the extant Order / Office Memorandum issued by DPIIT in this regard.
2. Seeking EMD submission from bidder(s), including via Additional Terms & Conditions, in contravention to exemption provided to such sellers under GeM GTC.
3. Publishing Custom / BOQ bids for items for which regular GeM categories are available without any Category item bunched with it.
4. Creating BoQ bid for single item.
5. Mentioning specific Brand or Make or Model or Manufacturer or Dealer name.
6. Mandating submission of documents in physical form as a pre-requisite to qualify bidders.
7. Floating / creation of work contracts as Custom Bids in Services.
8. Seeking sample with bid or approval of samples during bid evaluation process. (However, in bids for [attached categories](#), trials are allowed as per approved procurement policy of the buyer nodal Ministries)
9. Mandating foreign / international certifications even in case of existence of Indian Standards without specifying equivalent Indian Certification / standards.
10. Seeking experience from specific organization / department / institute only or from foreign / export experience.
11. Creating bid for items from irrelevant categories.
12. Incorporating any clause against the MSME policy and Preference to Make in India Policy.
13. Reference of conditions published on any external site or reference to external documents/clauses.
14. Asking for any Tender fee / Bid Participation fee / Auction fee in case of Bids / Forward Auction, as the case may be.
15. Any ATC clause in contravention with GeM GTC Clause 4 (xiii)(h) will be invalid. In case of multiple L1 bidders against a service bid, the buyer shall place the Contract by selection of a bidder amongst the L-1 bidders through a Random Algorithm executed by GeM system.

Further, if any seller has any objection/grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in the bid details field in Seller dashboard after logging in as a seller within 4 days of bid publication on GeM. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations.

This Bid is governed by the [General Terms and Conditions/सामान्य नियम और शर्तें](#), conditions stipulated in Bid and [Service Level Agreement](#) specific to this Service as provided in the Marketplace. However in case if any condition specified in General Terms and Conditions/सामान्य नियम और शर्तें is contradicted by the conditions stipulated in Service Level Agreement, then it will over ride the conditions in the General Terms and Conditions.

In terms of GeM GTC clause 26 regarding Restrictions on procurement from a bidder of a country which shares a land border with India, any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. While participating in bid, Bidder has to undertake compliance of this and any false declaration and non-compliance of this would be a ground for immediate termination of the contract and further legal action in accordance with the laws./जेम की सामान्य शर्तों के खंड 26 के संदर्भ में भारत के साथ भूमि सीमा साझा करने वाले देश के बिडर से खरीद पर प्रतिबंध के संबंध में भारत के साथ भूमि सीमा साझा करने वाले देश का कोई भी बिडर इस निविदा में बिड देने के लिए तभी पात्र होगा जब वह बिड देने वाला सक्षम प्राधिकारी के पास पंजीकृत हो। बिड में भाग लेते समय बिडर को इसका अनुपालन करना होगा और कोई भी गलत घोषणा किए जाने व इसका अनुपालन न करने पर अनुबंध को तत्काल समाप्त करने और कानून के अनुसार आगे की कानूनी कार्रवाई का आधार होगा।

---Thank You/धन्यवाद---