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	6th 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 - 12th December, 2024 Meeting link ID: 7571490712 Password: 684860 Join Meeting https://bharatvc.nic.in/join/7571490712
5	Last Date of Bid Submission.	1800 Hrs - 26th December, 2024
6	Technical Bid Opening Date	1830 Hrs - 26th 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. *Exception:* 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 beach 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 2nd 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 3rd 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 2nd iteration of testing	
E6		Carryout retesting of rectified defects and 3rd 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 words (Rupees…….....…….....……)		

* 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.lakshmidevarakonda@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	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

	22/23, Harmonized label, etc, including QR codes. 5. Allows booking of Domestic Money Orders across Counters and accessible by Internal Users (Department Employees).
Details for Site 2	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	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	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	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	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	1. Landing page containing the cards based on the roles of the user
Details for Site 8	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	1. All Payroll related activities. 2. All Pay reimbursement, and Advances activities with approvals.
Details for Site 10	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	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	1. Allows user creation, user authentication, access token generation, user enable/disable, event log maintenance, admin event log maintenance, and realm management. 2. Allows module card creation, role creation, role modification, role mapping, user enable, user disable, and Single sign-on. 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. 4. management of the Master data of Products, Offices, GL codes etc. 5. Dynamic QR Payment method is implemented for integrating with other solutions
Details for Site 13	1. Budget allocation and related activities. Budget allocation, proposal upload, expenditure plan upload etc is done using Excel upload. 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.
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	**Mail Booking (Domestic, International, EMO)** 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
Details for Site 2	**Pick-up & Induction** 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
Details for Site 3	**Transmission** 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
Details for Site 4	**Delivery & Recruitment Solutions** 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)

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---------->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 resting;
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 and 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 dev ices; 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 CERI-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 lo 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 l -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-ln may require through directions issued by it in exercise of powers vested in it by raw); 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 disbursal.

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

No.Tgy-50/13/2024-Technology-DOP
Government of India
Ministry of Communications
Department of Posts
(Tech. Division)

Dak Bhawan, Sandad Marg,
New Delhi – 110 001
Dated: 20.12.2024

CORRIGENDUM-1

The following corrigendum is issued in connection with the RFP for Information Security Audit & Performance Testing by CERT-In Empaneled Agencies published vide No.GEM/2024/B/5672506 on 06.12.2024.

<table>
<tr><th>Sl. No.</th><th>RFP Page Number, Clause Number</th><th colspan="3">Original Clause</th><th colspan="3">Revised Clause</th></tr>
<tr><td>1.</td><td>Page 54, Annexure 9 – Eligibility Criteria</td><td>S.No</td><td>Eligibility Criteria</td><td>Supporting Required</td><td>S.No</td><td>Eligibility Criteria</td><td>Supporting Required</td></tr>
<tr><td></td><td></td><td>3</td><td>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)</td><td>Audited Financial statements for the financial years 2021-22, 2022- 23 & 2023-24

Certified letter from the Chartered Accountant.</td><td>3</td><td>The Bidder must have registered an average annual turnover of Rs. 6 Crores or above (from Indian Operations only) in any 3 of the past 5 financial years i.e. FY2019-2020, FY 2020-2021, FY2021-22, FY2022-23 & FY2023-24 (Not inclusive of the turnover of associate companies)</td><td>Audited Financial statements for the financial years 2019-20, 2020-21, 2021-22, 2022- 23 & 2023-24

A certified letter from the Chartered Accountant.</td></tr>
<tr><td></td><td></td><td>4</td><td>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</td><td>Audited Financial statements for the financial years 2021-22, 2022- 23 & 2023-24

Certified letter from the Chartered Accountant.</td><td>4</td><td>The Bidder must be a Net profit-making entity (from Indian operations only) continuously in any 3 of the last 5 financial years, i.e. financial years – 2019-20, 2020-21, 2</td><td>Audited Financial statements for the financial years - 2019-20, 2020-21, 2021-22, 2022- 23 & 2023-24

A certified letter f</td></tr>
</table>

							021-22, 2022- 23 & 2023-24		rom the Chartered Accountant.	

2. Page 25, 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 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	

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	i. Work Order and Completion Certificate indicating the TPS count. ii. In case the TPS count is not mentioned in the Completion Certificate, a self-declaration on the bidder's company secretary stating the TPS count, along with the Completion Certificate, and providing the contact details of the
		>= 10	15	

									client who can be contacted to confirm the TPS-related information.
					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	i. Work Order and Completion Certificate indicating the TPS count. ii. In case the TPS count is not mentioned in the Completion Certificate, a self-declaration from the bidder's company secretary stating the TPS count, along with the Completion Certificate, and providing the contact details of the client
							>= 10	15	

									who can be contacted to confirm the TPS-related information. Note: In case a subcontractor is engaged for performance testing, the credentials of the subcontractor will be assessed for technical evaluation.
					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	i. Work Order and Completion Certificate indicating number of users ii. In case the number of users is not mentioned in the Completion Certificate, a self-declaration from the bidder's company secretary stating the number of users al
							>= 10	10	

								ong with the Completion Certificate, and providing the contact details of the client who can be contacted to confirm the details of the number of users
				4	Number of Performance Testing Conducted (Completed) in the last 36 months for Govt/PSU/Private for each application with more than 50 Lakhs registered users	>= 5 and < 10	5	i. Work Order and Completion Certificate indicating number of users ii. In case the number of users is not mentioned in the Completion Certificate, a self-declaration from the bidder's company secretary stating the number of users along with the Completion Certificate, and
						>= 10	10	

providing the contact details of the client who can be contacted to confirm the details of the number of users

Note: In case a subcontractor is engaged for performance testing, the credentials of the subcontractor will be assessed for technical evaluation.

3.	Page 27, Annexure 5 – Financial Bid	**Subject**: Financial Bid for Conducting Security Audit of DoP Application	**Subject:** Financial Bid for Information Security Audit & Performance Testing by CERT-In Empaneled Agencies.
4.	Page 26, Annexure 4 – Technical Bid Evaluation, point 7	No. of technical personnel with CISSP or ISMS (Ex. BS7799/ISO17799/ISO27001) Lead Assessor certification or any other information security qualifications	No. of technical personnel with CISSP or ISMS or CISA (Ex. BS7799/ISO17799/ISO27001) Lead Assessor certification or any other information security qualifications
5.	Page 3	Last Date of Bid Submission. 1800 Hrs – 26th December, 2024	Last Date of Bid Submission. 1600 Hrs – 6th January, 2025
6.	Page 3	Technical Bid Opening Date 1830 Hrs – 26th December, 2024	Bid Opening Date 1700 Hrs – 6th January, 2025

In addition, bidders may refer to the attached PDF file for a response to the pre-bid queries received.

This issues with the approval of Competent Authority.

Signed by Manoj Pragada
ADG (Tele)
Date: 20-12-2024 17:32:04

To

1. All concerned.
2. O/c.

Sl. No.	Bidder	Bidder's Query #	Page # from RFP	Clause #	Domain	RFP Clause	Query	DoP Response
1	TAC Security	1	54			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)	Our firm is Cert-In empaneled Limited company working in the cyber security field for past 10 years however our firm doesn't have Annual turnover of Rs. 10 Crore for FY 2021- 22 so kindly suggest whether our firm can form a Consortium	Consortium is not allowed, as per the RFP. However, bidders can sub-contract the 'Performance Testing' scope of work. Bidders may also note that the turnover criteria has been revised as follows: The Bidder must have registered an average turnover of Rs. 6 Crores or above (from Indian Operations only) in any 3 of the past 5 financial years i.e. FY2019-2020, FY2020-2021, FY2021-22, FY2022-23 & FY2023-24 (Not inclusive of the turnover of associate companies)
2	TAC Security	2	11			No Consortium is allowed	Kindly reconsider this criteria as it will enable Start-Up company like TAC Infosec Ltd to participate for this Bid.	Consortium is not allowed, as per the RFP. However, bidders can sub-contract the Performance testing scope of work.
3	Security Brigade	1				EMD of 60,00,000/-	Need Confirmation if MSME's are okay to bid without an EMD.	Please refer RFP page 6, section 11, pt. f for the clause on EMD exemption

4	Security Brigade	2				Project Mode	Does this project need to be executed onsite or remotely? In case of onsite, please share the location details.	Please refer RFP page 44, table 3.20 for the location details
5	Security Brigade	3				Revenue	Is it fine if the vendor does not have turnover more than 10 Cr?	Please refer RFP Annexure 9, 'Eligibility Criteria' Bidders may also note that the turnover criteria has been revised as follows: The Bidder must have registered an average turnover of Rs. 6 Crores or above (from Indian Operations only) in any 3 of the past 5 financial years i.e. FY2019-2020, FY2020-2021, FY2021-22, FY2022-23 & FY2023-24 (Not inclusive of the turnover of associate companies)
6	Security Brigade	4				Page 19 Section 8.2.1 : Clarification on TPS Requirements:	Can you provide more details on the expected transaction types and their respective volumes to ensure the 1500 TPS requirement is met?	Bidders may refer to Annexure 8 - 'Transaction Definition' for details of the types of transactions. However, exact volume of each transaction type cannot be shared.
7	Security Brigade	5				Concurrent Users	What is the expected number of concurrent users during peak load times? Please provide this information for each of the 17 websites/ web applications.	Performance Testing needs to be conducted to ensure 1500 concurrent users, and the number is same for all the 17 applications.

8	Security Brigade	6				Performance Metrics	Are there specific performance metrics or benchmarks that the applications must meet (e.g., response time, throughput, resource utilization)?	Bidder to propose as part of Approach & Methodology
9	Security Brigade	7				Test Environment	Will a dedicated test environment be provided, or will testing be conducted on the production environment?	Bidder will be provided a test environment, as per section 11.3, page 23 of the RFP
10	Security Brigade	8				Testing Method	Which testing method we need to opt for Web Applications/ Websites and Mobile Applications? White-Box/ Gray-Box or Black-Box	Bidder to propose as part of Approach & Methodology
11	Security Brigade	9				Test Environment	What are the specifications of the test environment (e.g., hardware, software, network configurations)?	Bidder will be provided a test environment, as per section 11.3, page 23 of the RFP.
12	Security Brigade	10				Data Availability	Will realistic test data be provided, or will we need to generate synthetic data for performance testing?	The successful bidder needs to generate the test data from the raw data supplied by DoP, please refer RFP page 21, section 10 'Project Milestones' for more details.
13	Security Brigade	11				Access and Permissions	What level of access will be provided to the performance testing team (e.g., administrative access, database access)?	Details of the testing environment shall be shared with the successful bidder during the test preparation phase.

14	Security Brigade	12				Integration Points	Are there any third-party integrations or APIs that need to be included in the performance testing?	As per RFP section 8.1.1, Pt. D, 'API Security Assessment', there will be following integrations: 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
15	Security Brigade	13				Performance Bottlenecks	Are there known performance bottlenecks or areas of concern that should be specifically addressed during testing?	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.
16	Security Brigade	14				Reporting Requirements	What format and level of detail are expected in the performance testing reports? Are there specific templates or standards that should be followed for reporting?	Bidder to propose as part of Approach & Methodology
17	Security Brigade	15				Iteration and Re-testing	How many iterations of performance testing and re-testing are expected after initial issue identification and remediation?	As per RFP, there shall be an initial assessment of application performance, followed by 2 iterations of retesting, and also performance testing for every change request

18	Security Brigade	16				Dependencies	Are there any dependencies or prerequisites that need to be addressed before performance testing can commence?	All the dependencies and prerequisites need to be identified by the successful bidder during test preparaation, and adressed during the test preparation phase
19	Security Brigade	17				Compliance Requirements	Are there any specific compliance standards or guidelines that the performance testing must adhere to (e.g., MeitY guidelines)?	Please refer RFP Annexure 7, 'MeitY Guidelines on Cybersecurity Audit', and global best practices.
20	Security Brigade	18				Security Considerations	Are there any security protocols or considerations that need to be taken into account during performance testing?	Please refer RFP section 8.2, 'Track 3 –Application Security Assessment for Change Requests', and global best practices.
21	Security Brigade	19				Point of Contact	Who will be the primary point of contact for any queries or issues that arise during the performance testing process?	Details of the point of contact shall be shared with the successful bidder.
22	Security Brigade	20				Collaboration Tools	Are there specific collaboration tools or platforms that will be used for communication and documentation during the project?	No specific tools
23	Security Brigade	21				Application scope	We understand that all the 17 applications in scope are web applications. Please confirm that there are no thick client applications to be tested in the scope of performance testing.	Please refer RFP Annexure 6, 'Technical Details of the Applications'

24	Security Brigade	22				Performance Requirements	Is the requirement to support a support a minimum of 1500 transactions per second for all the 17 applications in scope. If not please provide details of the specific applications for which this requirement is applicable.	Performance Testing needs to be conducted to ensure 1500 concurrent users, and the number is same for all the 17 applications.
25	Security Brigade	23				Mobile app testing	Is device level performance testing in scope or is it only at the web channel?	Performance testing needs to be conducted in the Datacentre environment through the web channel only.
26	Security Brigade	24				Mobile app testing	It is mentioned in Page 47 that the Mobile Application User Manual or SRS is attached. Please share the same for reference	User Manual/SRS shall be shared with the selected bidder
27	Security Brigade	25				Authentication	Is MFA authentication implemented for the application in scope of performance testing? If MFA authentication with Captcha is implemented, can we disable this authentication when we execute the performance test project?	Yes, MFA authentication is implemented for the application in scope of performance testing. Yes, this authentication can be disabled for executing the performance tests.
28	Security Brigade	26				Performance Monitoring	Are there any application performance monitoring tool in place? Please share the details and historical logs if available.	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.

29	Security Brigade	27				Applications	For the web version of the Applications, what browsers are supported?	As of date, this is the list Chrome 64+ Edge 79+ Firefox 67+ Opera 51+ Safari 12+
30	Security Brigade	28				Page 25 Annexure 4, Serial Number 2 and Serial number 4	We have partnered with a Tech Start-up to undertake the Performance Testing. As a part of the Technical Bid Evaluation criteria, we understand that Work Orders have been mentioned as Documentary Evidence for the Eligibility Criteria and Evaluation. As a young startup enrolled in the Startup India program we bring in the required expertise with experienced performance engineers who are well qualified and have carried out similar complex engagements. Please confirm if alternative forms of demonstrating our credentials can be accepted in lieu of work orders as documentary evidence.	Please refer RFP Annexure 4, 'Technical Bid Evaluation'

31	Security Brigade	29				Page 26. Annexure 4, Serial number 6: Skilled Technical Personnel	Due to the cyclical and sporadic nature of performance testing needs, we engage a large pool of skilled technical personnel on a consulting basis in addition to the full time employees on our payroll. As a young startup enrolled in the Startup India program and aiming to serve the needs of our Indian customers we utilize the core + flex model to cater to complex performance testing needs and offering the highest level of technical service. This also helps us bring in the best technical expertise as needed for complex engagements to cater to the contractual and service level obligations in complex engagements with our customers. In light of the above, we request your consideration in making an exception to the criteria stated in the RFP for startups that have been operational for less than 18 months.	Please refer RFP Annexure 4, 'Technical Bid Evaluation'

32	Security Brigade	30				Revenue	If overall company revenue is above 10CR for the last three years and can India specific operations revenue be less than 10cr?	Please refer RFP Annexure 9, 'Eligibility Criteria' Bidders may also note that the turnover criteria has been revised as follows: The Bidder must have registered an average turnover of Rs. 6 Crores or above (from Indian Operations only) in any 3 of the past 5 financial years i.e. FY2019-2020, FY2020-2021, FY2021-22, FY2022-23 & FY2023-24 (Not inclusive of the turnover of associate companies)

33	KPMG	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)	1.What are the key findings from the last security audit conducted by DoP? 2.How does DoP handle incidents of security breaches or data leaks? 3.What measures are in place for continuous monitoring and improvement of security policies?	1. Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing. 2. DoP has a comprehensive ISMP and CCMP to handle such incidents, the policy will be shared with the successful bidder. 3. DoP has a comprehensive ISMP and CCMP for continuous monitoring and improvement, the policy will be shared with the successful bidder.
34	KPMG	2	Page 17_ PDF 1733491448		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	1. Is the DOP ISO 27001 certified? 2. Does DOP follow ISO 27001 guidelines related to security policy and procedure mantaince? 3. What is the frequency of Policy review in DOP 4. Please indicate the list of policies, procedures and guidelines which needs to be reviewed. 5. What is the process of performing risk assessment in DOP?	1. Details will be shared with the successful bidder. 2. Details will be shared with the successful bidder. 3. As per Govt of India regulations, DoP updates it policy as and when the need arises. 4. Details will be shared with the successful bidder. 5. Details will be shared with the successful bidder.

						Assessment and Remediation vii. Problem Management viii. Risk Assessment ix. Backup and Restoration		

35	KPMG	3	Page 17_ PDF 1733491448		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	1. Does DOP perform internal Configuration review? If yes, what is the frequency? 2. What SIEM , PIM DAM tools are used in DOP. 3. Does DOP perform internal configurations reviews? If yes, what is the frequency? 4. How often are network and security architecture reviews conducted? 5. What are the criteria for selecting security tools like WAF,IPS, IDS and firewalls? 6. Are there any specific compliance requiremens that the network configuration must adhere to?	1. Details will be shared with the successful bidder once the application goers live. 2. Details will be shared with the successful bidder once the application goers live. 3. Details will be shared with the successful bidder once the application goers live. 4. Details will be shared with the successful bidder once the application goers live. 5. Details will be shared with the successful bidder once the application goers live. 6. Query not clear.

36	KPMG	4	Page 17 and 18_ PDF 1733491448		Network Configuration Assessment	VAPT should be comprehensive but not limited to following activities: i. Injection ii. Broken Authentication and Session Management 18 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,	1.Please clarify if the VAPT can be performed remotely through the bidder's lab or if it has to be performed onsite. 2. How are the results of VAPT communicated to the relevant stakeholders? 3. What is the process for addressing and mitigating identified vulnerabilities?	1. Please refer RFP page 44, table 3.20 for the location details 2. Through email 3. As per the RFP

						which are vulnerable to the Applications		

37	KPMG	5	Page 18_ PDF 1733491448		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	1. What are the specific security measures in place for the APIs designed for the APIs designed for data exchanges within and outside the CBIC environment? 2. How often is the security assessment of the APIs conducted? 3. What are the common vulnerabilities identified in previous API security assessments? 4. How does DOP ensure the security of data exchanges between different applications and external entities? 5. Are there any specific standards or frameworks followed for API security? 6.What are the specific requirements for API security testing? Should it include testing for common vulnerabilities such as broken authentication, data exposure, and rate limiting? 7.How many APIs need to be tested, and what are their endpoints?	1. App Key, MFA and per API authZ, AuthN with JWT token. CBIC to be read as DoP 2. As per the RFP requirements. 3. Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing. 4. DoP has a comprehensive ISMP policy which ensures the security of data exchanges between different applications and external entities 5. Yes, https and mTLS in addition to point no 1 6. Bidder to adhere to MeitY Guidelines on Cybersecurity Audit (refer Annexure 7) and other global best practices. 7. As per RFP section 8.1.1, Pt. D, 'API Security Assessment', there shall be maximum 500 APIs

						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		

38	KPMG	6	Page 18_ PDF 1733491448		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	1. Are there specific containment measures tested for cloud infrastructure security? 2. What are the key chanllenges faced in securing cloud infrastructure? 3. How does DOP ensure compliance with data protection regulations in the cloud environment?	1. Not applicable - These are new applications developed under IT 2.0 and have not been rolled out yet. 2. Not applicable - These are new applications developed under IT 2.0 and have not been rolled out yet. 3. DoP has a comprehensive ISMP policy which ensures the security of data exchanges between different applications and external entities

						xii. Lockout Testing xiii. Man in the Middle attack xiv. Containment Measure Testing 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		

39	KPMG	7	PDF 1733491448_Page 25		Technical Bid Evaluation	Number of Audits Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with TPS > 1500	The completion Certificate issued by all the entities (whether Govt/PSU/Private), does not mention the TPS count of the application audited. Request to kindly elaborate this clause	Bidder may submit a self-declaration from the company secretary stating the contact details of the client who can be contacted to confirm the TPS related details
40	KPMG	8			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.	1.Can the penetration testing be performed remotely, or is onsite testing required? 2.Are there any specific tools or methodologies preferred for conducting penetration testing? 3.What are the critical systems and applications that need to be included in the penetration testing scope? 4. Is there a process in place for validating the effectiveness of the implemented patches and remediation measures? 5.Will the penetration testing be conducted on a live production environment, or will a separate staging environment be provided?	1. Please refer RFP page 44, table 3.20 for the location details 2. Bidder to propose 3. As per the RFP 4. Yes, Change Approval Board(CAB) mechanism is proposed in the SI RFP. 5. Testing environment to be provided by DoP, refer section 10 'Project Milestones' for details.
41	KPMG	48	N/A				Is Performance testing of reports will also be in scope?	Yes, as per the RFP

42	KPMG	1	Page 17_ PDF 1733491448		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	Has DOP followed ISO 27001:2022 guidelines for drafting of their security policy and procedure and mantaince?	Details will be shared with the successful bidder.

43	KPMG	2	Page 17_ PDF 1733491448		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	1. What SIEM , PIM DAM tools are used in DOP. 2. Can DOP share an estimated number of Network devices in order for the bidder to evaluate their pricing effectively.	1. Details will be shared with the successful bidder once the application goers live. 2. These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.

44	KPMG	3	Page 17 and 18_ PDF 1733491448		Network Configuration Assessment	VAPT should be comprehensive but not limited to following activities: i. Injection ii. Broken Authentication and Session Management 18 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,	Please clarify if the VAPT can be performed remotely through the bidder's lab or if it has to be performed onsite.	Please refer RFP page 44, table 3.20 for the location details

						which are vulnerable to the Applications		
45	KPMG	4	PDF 1733491448_Page 25		Technical Bid Evaluation	Number of Audits Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with TPS > 1500	The completion Certificate issued by all the entities (whether Govt/PSU/Private), does not mention the TPS count of the application audited. Request to kindly elaborate this clause.	Bidder may submit a self-declaration from the company secretary stating the details of client as well as a contact person at the client' end, who can be contacted to confirm the TPS related details

46	KPMG	5	Page # 7		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.	Need more clarification that the payment will be released after one time audits and CRs for all the applications both.	Query not clear
47	KPMG	6	Page # 8		Service Level Agreeme nt	3. Completion of deliverables under Security Audit and Performance Testing Agency	What in the case, if delay will happen because of any other party other than Security Audit and Performance Testing Agency ?	Any delays in exection of the project, which is not attributable to the bidder, will not affect the payments for the bidder.
48	KPMG	7	Page # 9		Service Level Agreeme nt	Penalties shall be capped to 10% of the annual payment of the total contract value.	Does that line means minimun penalty is 0.5% and maximum penalty is 10% ?	Please refer RFP Section 14 'Service Level Agreement'
49	KPMG	8	Page # 16		Annexure 2 – Scope of Work	3. List of Tasks to be conducted for Information Security Audit and Performance Testing c. Application/Datab ase Performance Testing	What type of performance testing should be performed? E.g. Load Test, Volume testing	Bidder to propose

50	KPMG	9	Page # 19		8.2.1.Initial Performance Testing	(Refer to Annexure 7 for the definition of a transaction)	For the definition of transaction, need to refer Annexure 7 OR Annexure 8 ?	Bidders may refer to annxure 8 for the transaction definition
51	KPMG	10	Page # 22		11.1. Test Preparation/Design	1. Identification of business functionalities for testing from in-scope modules/interfaces	How much time is planned for identification of business functionalities and when will it happen ?	Please refer RFP section 10 'Project Milestones, on page 21
52	KPMG	11	Page # 22		11.1. Test Preparation/Design	2. Develop detailed end-to-end business scenarios that will be tested based on 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	Please comfirm that top 100 scenarios will be considered from all web applications and mobile applications and the final scope will be top 100 scenarios only for M1 and M2.	As per RFP Section 11.1

53	KPMG	12	Page # 22		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	Testing techniques mentioned are more related to functional testing. Does the performance testing team need to create the test cases for top 100 scenarios on the basis of each testing technique ?	Bidder to propose the test strategy. The testing requirements shared as part of the RFP are only broad expectations from the bidder.

						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		

54	KPMG	13	Page # 23		11.3. Test Execution	2. Prepare test data using raw data provided by DoP	In what format test data will be provided ? What about accuracy of test data ? In case of bad data or delay in receiving the test data, what about the mitigation and buffer timelines ?	As per RFP, Section 10 'Project Milestones', test data preparation is the responsibility of the bidder as part of Milestone M1.
55	KPMG	14	Page # 23		11.3. Test Execution	3. Execute test cases (SRS/ design documents etc. of each of the core processes needs to be shared by DoP)	Please confirm, Only performance test cases for top 100 scenarios are in scope not functional test cases.	Bidder needs to cover all the testing types for the top 100 test cases identified, as per RFP requirements.
56	KPMG	15	Page # 23		11.3. Test Execution	4. Verify software functionality in compliance with the specified functional & non-functional requirements as mentioned in the SRS.	Please confirm, Only performance test cases for top 100 scenarios will be executed as per the SRS.	Bidder needs to cover all the testing types for the top 100 test cases identified, as per RFP requirements.
57	KPMG	16	Page # 23		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.	Performance testing team will not be responsible for defect fixing.	Query not clear

58	KPMG	17	Page # 23		11.5. Defect Verification & Re-Testing	6. Provide solution for remediation of the issues reported are due to functional or used software	Need more clarification what kind of solution for remediation is expected from Performance testing team.	As per RFP section 11.5. Defect Verification & Re-Testing
59	KPMG	18	Page # 27		Annexure 5 – Financial Bid	Subject: Financial Bid for Conducting Security Audit of DoP Application	Only security audit is mentioned and not the performance testing. Shouldn't performance testing also included in subject ?	Accepted. Please refer to corrigendum
60	KPMG	19	Page # 27		Annexure 5 – Financial Bid	Multiplying Factor	What is multiplying factor, particularly in the case of Change requests ? Is 500 is maximum number of change requests in an year for all applications ?	As per RFP, 500 is a tentative number of change requests for 5 years.
61	KPMG	20	Page # 37		3.6) Number of Roles in the Application	N/A	Roles cell is blank for Details for Site 17. Please update the same.	4 roles.
62	KPMG	21	Page # 38		3.7) Number of static pages	N/A	Static Pages cell is blank for Details for Site 17. Please update the same.	No static pages for BCP management portal
63	KPMG	22	Page # 38		3.8) Number of Dynamic Pages	N/A	Dynamic Pages cell is blank for Details for Site 17. Please update the same.	BCP applications uses thick client on desktops , mobile / tablet apps. Only BCP management portal encompasses 7 dynamic pages

64	KPMG	23	Page # 38		3.9) Number of User Input fields (approximately)	N/A	Number of User Input fields cell is blank for Details for Site 17. Please update the same.	User i/p fields on BCP management portal come to 30

65	KPMG	24	Page # 39 - 45		3.10), 3.11). 3.12),3.14) 3.15), 3.16), 3.20), 3.22) 3.25), 3.26), 3.27)	N/A	Cell is blank for Details for Site 17. Please update the same.	Operating System details with version BCP thick client Windows 10, 11 BCP Portal Ubuntu 22.04.4 LTS BCP Mobile/Tablet Android Web server details with version BCP Solutions Apache , nginx Bck end Postgres Version:16 BCP thick Client - Desktop Windows Sqlite BCP Mobile Application Sqlite Front-end tools/Server-Side Scripts/Programming tools used with version de BCP Solutions - Management Portal ReactJS, NextJS, Golang Desktop Window app , Mobile/Tablet Android app Flutter Document/report details HTML, PDF, XML et HTML

66	KPMG	25	Page # 44		3.24) Please share SRS or technical documents	N/A	Cell is blank for Details for Site 15, 16 & 17. Please update the same.	All the blanks may be treated as Yes.
67	KPMG	26	Page # 48		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);	How many web applications have both thick and thin client ?	Device Registration App, Dak Sewa Mobile App, Internal Mobile App
68	KPMG	27	Page # 48		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);	How the thick clients can be accessed ?	The BCP application details will be provided prior to the engagement.

69	KPMG	28	N/A		N/A	N/A	What is the protocol between client and server for web applications and mobile applications? E.g. http, https, TCP, FTP	HTTPS
70	KPMG	29	N/A		N/A	N/A	How many number of total users expected to access the application in real time ?	Approximately 1 lakh users
71	KPMG	30	N/A		N/A	N/A	What is the number of simultaneous users / Concurrent users ?	As per RFP, section 8.2 'Application Performance Testing'
72	KPMG	31	N/A		N/A	N/A	What are the different type of requests and requests / sec ? (e.g. for a scenario X, Login : 2500 request/s , Search : 5000 requests/s ,Logout : 2500 requests/s)	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.
73	KPMG	32	N/A		N/A	N/A	What is the desired network bandwidth desired (in Mbps) ?	Query not clear
74	KPMG	33	N/A		N/A	N/A	What is the maximum number of records in any database ?	Approximately around 100 Crore
75	KPMG	34	N/A		N/A	N/A	How many transactions are expected/second	As per RFP, section 8.2 'Application Performance Testing'
76	KPMG	35	N/A		N/A	N/A	Please confirm if you have dedicated Test Environment.	Yes
77	KPMG	36	N/A		N/A	N/A	Which Application server is running with the system?	Node.js and Go server

78	KPMG	37	N/A		N/A	N/A	How do they access the application(type of application in scope)? E.g. RDP or Web or mobile?	Web and Mobile
79	KPMG	38	N/A		N/A	N/A	Is the test environment a replica of production environment ?	Details of the testing environment shall be shared with the successful bidder during the test preparation phase.
80	KPMG	39	N/A		N/A	N/A	Is the DB volume of test environment and production environment similar ?	Details of the testing environment shall be shared with the successful bidder during the test preparation phase.
81	KPMG	40	N/A		N/A	N/A	Do you have traffic monitoring tool deployed on web server? E.g. Google Analytics, New Relic etc.	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.
82	KPMG	41	N/A		N/A	N/A	Is any application required any VPN to connected to test environment/Production enviornment?	Details of the testing environment shall be shared with the successful bidder during the test preparation phase.
83	KPMG	42	N/A		N/A	N/A	Are there any known issue(s) in the web applications and mobile applications ? E.g.Memory lock , Higher CPU and Memory utilization , Unexpected growth in daily visitors ,More response time which leads to time out error	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.

84	KPMG	43	N/A		N/A	N/A	Is the development team available to make the necessary configuration for performance test ?	Query not clear
85	KPMG	44	N/A		N/A	N/A	Do you have a server monitoring team, to monitor the server stats during load generation?	N/A
86	KPMG	45	N/A		N/A	N/A	Is Performance testing of reports will also be in scope? If yes, please share the approximate no of reports.	Yes, plase refer to Corrigendum.
87	KPMG	46	N/A		N/A	N/A	Is the web URL availabe for mobile applications ?	Yes
88	KPMG	47	N/A		N/A	N/A	Can the performance testing be done remotely, Is there any VPN connection available ?	Please refer RFP page 44, table 3.20 for the location details
89	AQM Technologies	1	NA	General		Performance Testing	Please provide the list of all applications to be tested for Performance/Load Testing	As per RFP Annexure 6, 'Technical Details of the Applications'
90	AQM Technologies	2	NA	General		Performance Testing	Please provide the frequency of Performance testing needed (once a year, twice a year, etc)	As per RFP, there shall be an initial assessment of application performance, followed by 2 iterations of retesting, and also performance testing for every change request
91	AQM Technologies	3	NA	General		Performance Testing	Please provide the expected load w.r.t. concurrent users & expected TPS across all applications in scope for performance testing	As per RFP Annexure 6, 'Technical Details of the Applications', there will be 1500 concurrent users

92	AQM Technologies	4	NA	General		Performance Testing	Please provide the maximum concurrency to consider for performance testing across any given application list to estimate for Performance testing tool licenses	As per RFP Annexure 6, 'Technical Details of the Applications', there will be 1500 concurrent users
93	AQM Technologies	5	NA	General		Performance Testing	Please provide the details of all applications in-scope for Performance/Load Testing w.r.t. Type (e.g. web based, Mobile Based or APIs)	Bidders may refer to annexure 6 for the technical details of the application
94	AQM Technologies	6	NA	General		Performance Testing	Please provide the details of all applications in-scope for Performance/Load Testing w.r.t. protocols for communication between client & server (e.g. HTTP/HTTPS based, TCP socket, etc.)	Please refer RFP Annexure 6, 'Technical Details of the Applications'
95	AQM Technologies	7	NA	General		Performance Testing	Any Performance Testing tool currently in use in the organisation which the performance testing team can utilise? (e.g. Loadrunner, Jmeter)	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.
96	AQM Technologies	8	NA	General		Performance Testing	Any Performance Monitoring tool (APM tools for RCA) currently in use in the organisation which the performance testing team can utilise? (e.g. Appdynamics, Dynatrace)	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.

97	AQM Technologies	9	NA	General		Performance Testing	Preference of tools Performance Testing & Monitoring tools (Open source or commercial Or open to any)	Bidder to propose
98	AQM Technologies	10	NA	General		Performance Testing	Preference of tools Performance Testing & Monitoring tools w.r.t. On-Prem OR cloud-based	Bidder to propose
99	AQM Technologies	11	NA	General		Performance Testing	Share server details of all the applications to estimate for monitoring tool implementation efforts. Share Count, OS, Server-type (e.g. 5 servers, Linux OS, Weblogic server) for all web, app & DB servers	Details will be shared with the successful bidder once the application goers live.
100	AQM Technologies	12	NA	General		Performance Testing	Confirm that Load generator machines will be provided by DoP to install Performance testing tools & execute tests	Bidder will be provided a test environment, as per section 11.3, page 23 of the RFP
101	AQM Technologies	13	NA	General		Performance Testing	Confirm the project execution model for performance testing (onsite at Delhi, OR offshore Access will be provided)	Please refer RFP page 44, table 3.20 for the location details
102	AQM Technologies	14	NA	General		Performance Testing	Confirm if there will be any efforts of stub creation or service virtualisation (during performance testing) to bypass any third-party calls Or will this be handled by DoP development team	Query not clear

103	AQM Technologies	15	NA	General		Performance Testing	Please confirm that how many applications can be performance tested at any given instant in a month (max count of expected performance test audits in a month)	The number of application performance audits will depend on the change requests in a given month. Hence, the exact number of such audits cannot be ascertained.
104	AQM Technologies	16	3	8		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	Requesting to allow submission of EMD in the form of 'Performance Bank Guarantee (PBG)' for such large amount	As per the RFP page 3, table 'Important Dates', pt. 8

105	AQM Technologies	17	6	11. EMD		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.	Requesting to exempt MSME vendors from EMD submission	Please refer RFP page 6, section 11, pt. f for the clause on EMD exemption
106	AQM Technologies	18	7	13		Payment Terms	Requesting to add clause for MSME vendor 'Payment will be made to vendors within 45 Days of submission of Tax Invoice'	No change

107	AQM Technologies	19	11	22		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.	Requesting to modify this clause as 'Either party may, by written notice of 60 (sixty) days sent to the other party, terminate the Agreement, in whole at any time for its convenience. The notice of termination shall specify that termination is for the either party's convenience, the extent to which the performance of work under the Agreement is terminated, and the date upon which such termination becomes effective.'	No change
108	AQM Technologies	20	19	8.2. Track 2 – Application Performance Testing		General	Kindly share the current tools used by DoP for Performance Testing. Also, please confirm if the Test Cases & scripts can be extended for reusability to the selected bidder	Not applicable - These are new applications developed under IT 2.0 and shall be moved to production post completion of Security Audit & Performance testing.

109	AQM Technologies	21	25	Annexure 4 – Technical Bid Evaluation		1. Number of Audits Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with TPS > 1500	Kindly confirm if TPS & concurrent user have same meaning here	As per RFP, section 8.2 'Application Performance Testing'
110	AQM Technologies	22	25	Annexure 4 – Technical Bid Evaluation		1. Number of Audits Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with TPS > 1500 2. Number of Performance Testing Conducted (Completed) in last 36 months for Govt/PSU/Private for each application with TPS > 1500	Kindly confirm if the understanding is correct: If 4 Audit/Performance test conducted for same application, will be counted as 4 projects & submission of Work order for the same is allowed	As per the RFP, Annexure 4 'Technical Bid Evaluation', each application will be counted as one project.
111	AQM Technologies	23	25	Annexure 4 – Technical Bid Evaluation		Documentary Evidence - 1. Work Order and Completion Certificate indicating TPS Count 2. Work Order and Completion Certificate indicating Number of Users	1: Requesting to accept Audit/Test report/client credentials as evidence along with Work Order 2: Since Number of Users count is a confidential information for the client companies, please accept the Work order/credentials without the user details and TPS details	1. No change, as per the RFP 2. Bidder may submit a self-declaration from the company secretary stating the contact details of the client who can be contacted to confirm the TPS and concurrency related details

112	AQM Technologies	24	27	Annexure 5 – Financial Bid		General	Kindly confirm the understanding of the calculation: Frequency*Mulliplying Factor*Unit Rate = Amount (Rs.)	Multiplying Factor * Unit Rate = Amount (Rs.)
113	AQM Technologies	25	54	Annexure 9 – Eligibility Criteria		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.	Requesting to modify this clause as 'The Bidder should be empanelled by CERT- In as well as STQC 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.' Since it is mandate by MeitY under the 'Application Development & Re-Engineering Guidelines' (https://www.meity.gov.in/writereaddata/files/Application_Development_Re-Engineering_Guidelines_0.pdf)	No change
114	AQM Technologies	26	16	8.1		Annexure 2- Scope of Work	Please provide the DC and DR locations for the audit.	Please refer RFP page 44, table 3.20 for the location details

115	AQM Technologies	27	16	8.1		Annexure 2- Scope of Work	Please confirm whether the expected security testing approach is Black Box or Grey Box.	Bidder to propose as part of Approach & Methodology
116	AQM Technologies	28	17	8.1.1 (b,e)		b: Network Configuration Assessment e: Cloud Infrastructure Assessment	Please provide the digital inventory for the Infrastructure/Network Configuration Assessment and Vulnerability Assessment and Penetration Testing (VAPT). Kindly ensure that the inventory includes an approximate count of the devices within the scope of the assessment.	Details will be shared with the successful bidder once the application goers live.
117	AQM Technologies	29	18	8.1.1 (d)		APIs Security Assessment	Please confirm whether the count of 500 refers to the number of APIs or endpoints. We assume a one-to-one relationship, meaning 500 APIs correspond to 500 endpoints (1 endpoint for 1 API).	Selected bidder shall be required to undertake the assessment as per the RFP. The count refers to only APIs.
118	AQM Technologies	30	18	8.1.1 (c,d)		c: Application security Assessment d: APIs Security Assessment	Please confirm the count of applications and APIs for the Secure Code Review. Additionally, confirm whether the source code of the APIs is included in the application's source code or treated separately.	As per RFP Annexure 6, 'Technical Details of the Applications'. There are about 500 APIs apart from the applications listed in the RFP.

119	AQM Technologies	31	19	8.1		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.	Please confirm if the process involves 1 initial round of testing and 2 revalidation rounds, where only the closure of vulnerabilities reported in the initial round will be tested. Also, confirm that the revalidation rounds do not require conducting the entire VAPT, only validation of previously reported issues in initial round.	Selected bidder shall be required to undertake the assessment as per the RFP and revalidation needs to be conducted only for the identified issues.
120	AQM Technologies	32	26	Annexure 4 – Technical Bid Evaluation		No. of technical personnel with CISSP or ISMS (Ex. BS7799/ISO17799/ISO27001) Lead Assessor certification or any other information security qualifications	Please let us know if CISA or other similar domain related certification can be considered in place of CISSP or ISMS.	Accepted.
121	AAA Technologies	1	1			GEM Bid - Bid End Date/Time/ 27-12-2024 20:00:00	a) We request you to kindly extend the bid submission date till 6th January 2025	Noted, DoP will decide about extension at appropriate time and intimate the same to all bedders through GeM/ Indiapost Portal.

122	AAA Technologies	2	19			8.2. Track 2 – Application Performance Testing	a) We are a CERT-IN accredited organization. According to CERT-IN, audit firms can undertake security audits but not performance testing.Performance testing is performed by the firm that develops the application, and these scopes apply to those firms rather than CERT-In empanelled firms. Our request is that you float two separate RFPs for application testing and performance testing. The security company will be unable to provide work orders for performance testing. Please provide a solution so that we can participate in the tender. As it is mentioned no consortium is allowed in page number 10 of RFP b) Location of audit required for each activity mentioned in RFP	a) As per the RFP, sub contracting has been allowed for the performance testing scope of work. In case a subcontractor is engaged, the subcontractor's credentials will be considered for the technical evaluation. b) Please refer RFP page 44, table 3.20 for the location details