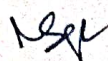
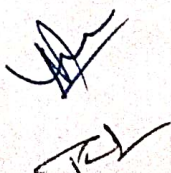
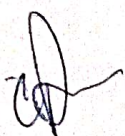
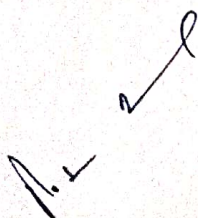


**Government of NCT of Delhi
Delhi e-Governance Society
Department of Information Technology,
8th Level, B-Wing, Delhi Secretariat, IP Estate,
New Delhi-110002**

Request for Proposal

**To select a Cyber Security Agency to
conduct Security Audit for IT System of
GNCTD**

This RFP is to provide manpower for Security Auditing of the IT Systems currently running or will be built in due course of time by various departments/local bodies/autonomous bodies of Government of NCT of Delhi.



Fact Sheet:

RFP Issued By	Delhi eGovernance Society, Department of Information Technology, GNCT of Delhi
Selection Method	Bidder will be selected using Lowest Qualifying Financial Bid (L1) amongst the technically qualified bids.
Availability of RFP	By e-Mail / Website
EMD/Bid Security	<p>Earnest Money Deposit (EMD) of amount of Rs. 2,00,000/- (Two lakhs only) shall be in the form of Demand Draft / Bankers' Cheque / Unconditional Bank Guarantee from any of the Nationalized Scheduled Commercial Bank in original physical form, drawn in favour of Delhi e-Governance Society, GNCTD, payable at Delhi at 8th Level, B wing, Delhi Secretariat, IP Estate, New Delhi on or before last date and time of submission of bid proposal.</p> <p>Bidders shall be eligible for benefits under Revised Rule 170(i) of GFR, 2017 upon submission of appropriate document. To be submitted in lieu of EMD.</p>
Date of Publishing of Tender	Date 03.01.2025 at 5:00 PM
Pre Bid Meeting	<p>09.01.2025 at 11:30 AM .Pre bid meeting link will shared to the registered bidder.</p> <p>For registration for the Pre-bid meeting, the participants is required to share the Name, email address, Designation and company name to Smt. Mamta Sharma at mamta.sharma22@delhi.gov.in in one day before the Pre-bid with the subject line of the email as "Clarification on bid published for hiring Cyber Security Agency"</p>
Issue of Addendum/Corrigendum (if any)	16 .01.2025 or the date decided by the DeGS
Date and Time of Opening of Bids – Pre Qualification	21.01.2025 at 11:00 AM
Place of Opening of Bids	DeGS, 8th Level. B Wing, Delhi Secretariat, IP Estate New Delhi 110003

Note: This bid document is not transferable.

Sd/-
Member Secretary (DeGS)

Disclaimer

The information contained in this Tender Document or subsequently provided to Bidder(s) or Applicants whether verbally or in documentary form by or on behalf of Member Secretary, DeGS, GNCTD, is provided to the Bidder(s) on the terms and conditions set out in this Tender Document and all other terms and conditions subject to which such information is provided.




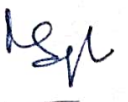

This Tender Document is not an agreement and is not an offer or invitation by the Member Secretary, Delhi e-Governance Society, GNCTD to any party other than the Applicants who are qualified to submit the Bids ("Bidders"). The principle of this Tender Document is to provide the Bidder(s) with information to support the formulation of their Proposals. This Tender Document does not purport to contain all the information each Bidder may entail. This Tender Document may not be apposite for all bidders, and it is not possible for the Member Secretary (DeGS), to consider the investment objectives, financial situation, and particular needs of each Bidder who reads or uses this Tender Document. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this Tender Document and where necessary, obtain independent advice from appropriate sources. The Member Secretary (DeGS), makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the precision, reliability or completeness of the Tender Document. The Member Secretary (DeGS) may in his absolute discretion, but without being under any obligation to do so, update, improve or supplement the information in this tender document.

Contents

Section 1: Introduction	7
1.1 Preface	7
1.2 Objective	7
Section 2: Request for Proposal	8
2.1 Due Diligence	8
2.2 Cost of Bidding	8
2.3 Content of Bidding Document	8
2.4 Clarification of Bidding Documents	8
2.5 Amendment of Bidding Documents	9
Section 3: Instructions to Bidder (ITB)	9
3.1 Preparation of Bids	9
3.1.1 Language of Bid	9
3.1.2 Pre-Qualification Proposal	9
3.1.3 Financial Bid	10
3.1.4 Undertaking	10
3.2 Quoting for Bid Prices	10
3.2.1 Prices in the Price Schedule	10
3.2.2 Fixed Price	10
3.2.3 Bid Currencies	10
3.3. Bid Security	10
3.3.1. Amount of Bid Security	10
3.3.2. Discharge of Security Bid of Unsuccessful Bidder	11
3.4. Period of Validity of Bids	11
3.4.1. Validity Period	11
3.4.2. Extension of Period of Validity	11
3.4.3. Submission of Bid	11
3.4.4. Mailing Address for EMD of Bids	11
3.4.5. Rejection of Bid	12
3.4.6. Extension for Last date for Submission	12
3.4.7. Bid Opening and Evaluation of Bids	12
3.4.8. Pre-qualification, Evaluation and Comparison of Bids	13
3.4.9. Contacting the Client	13
3.5. Issue of Work Order & Signing of Contract	13

3.5.1.	Client's right to accept any Bid and to reject any Bid or all Bids	13
3.5.2.	Notification of Award (Letter of Intent (LOI))	13
3.5.3.	Signing of agreement	13
3.5.4.	Expenses for the Contract	13
3.5.5.	Failure to abide by the Agreement	13
3.5.6.	Performance Guarantee	13
3.5.7.	Terms of Payment	14
3.5.8.	No Claim Certificate	14
3.5.9.	Termination	14
3.5.10.	Standard of Performance	15
3.5.11.	Penalties	15
3.5.12.	Force Majeure	15
3.5.13.	Arbitration and Jurisdiction	16
3.5.14.	Blacklisting	16
3.5.15	Contract Period	16
3.6.	Time line :	16
Section 4 - Scope of work to be included		16
4.1.	Suggestive Methodology for Vulnerability Assessment	17
4.1.1.	Threat Identification	17
4.1.2.	Threat-Source Identification.	17
4.1.3.	Vulnerability Identification	17
4.1.4.	Penetration Testing (PT)	19
4.1.5	Network Audit	19
4.1.6	Mobile App Audit	20
4.2.	Responsibility of the Bidder	20
4.2.1.	Responsibilities	20
4.2.2.	Standard Activities to be performed	21
4.2.4	Security Testing Types	22
	Web Application Security Testing	22
	Mobile Application Security Testing	22
4.3.	Documentation	22
Appendix 1: Pre-qualification Criteria		24
	Form A: Bid Application Sheet	25
	Form B: Undertaking	26

Form C: Warranty	27
Appendix II: Content and Format of Financial Bid	28
Appendix III: List of Applications to be Audited/rectified	29
Appendix IV : CERT –IN Format of reporting Vulnerability (Indicative)	31

Section 1: Introduction

1.1 Preface

The popularity of IT Systems has grown dramatically, with many organizations converting legacy mainframe and database systems into dynamic web applications/Mobile Applications. Technologies such as PHP, Ajax, JavaScript, JSP, Java, ASP, ASP.NET, Cold Fusion, Perl, Flash, Ruby, NODEJS, Flatter etc allow a company to quickly develop client-server applications that can be accessed over the internet and/or intranet.

With the growth of web-enabled applications, mobile apps, Web Services etc attacks and threats have become more sophisticated. The Vendor will have to provide with web application security service to keep the applications of Delhi Government ahead of the curve through constant innovation and evolution.

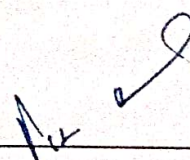
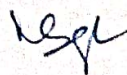
1.2 Objective

The objective of this RFP is to engage an appropriate qualified service providing company for Security Auditing and Quality Auditing of IT systems (as per **CERT-In**, NIC and other Government of India guidelines) currently running in all departments/local bodies under Government of NCT of Delhi and new upcoming applications to be built in due course of time, by deploying qualified resources/team with backend support of organization knowledge and strength.

Only current CERT-IN empanelled agencies with their registered or branch offices in the Delhi NCR region can participate in this tender. The selected bidder will have to follow the security auditing guidelines (issued by CERT-IN, NIC, STQC, DIT-GOI, MHA and other Government agencies). Empanelment of the security auditing organisation/agencies shall be valid for ~~minimum~~ next 02 years from the date of award of the bid.

The deployed resources/team will be empowered with organization knowledge & strength and they will also provide possible solutions to the department in fixing the vulnerabilities as and when identified by them during the tenure.

The scope will not only be limited to the Security Auditing of the applications but also to provide suggestions to fix the vulnerabilities that would be reported during the Audit. The Audit and vulnerability fixing of the identified threats would be an ongoing process till the tenure.



Section 2: Request for Proposal

2.1 Due Diligence

The Bidder is expected to examine all instructions, forms, terms & conditions and specifications in the bidding document along with all relevant guidelines issued by CERT-In, NIC and Government of India time to time. The bid should be precise, complete and in the prescribed format as per the requirement of the bid document. Failure to furnish all information required as per bid document may be treated as non-responsive and **liable to be rejected**.

2.2 Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its bid and DeGS, GNCTD hereinafter referred to as "the Client", will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

2.3 Content of Bidding Document

The requirements, bidding procedures and contract terms are prescribed in the bidding documents. The bidding documents include:

Appendix - I: Pre-Qualification Criteria

Appendix - II: Content and format of Financial Bid along with Evaluation Criteria

Appendix - III: Tentative List of existing Web Applications

2.4 Clarification of Bidding Documents

A prospective Bidder requiring any clarification shall have to register themselves before being allowed access to the meeting. For registration for the Pre-bid meeting, the participants is required to share the Name, email address, Designation and company name to Smt. Mamta Sharma at mamta.sharma22@delhi.gov.in in one day before the Pre-bid with the subject line of the email as "Clarification on bid published for hiring Cyber Security Agency". Purchaser may not allow any unregistered email id or participants.

The Bidders will have to ensure that their queries (in **Excel format**) for Pre-Bid meeting should reach to email id: **mamta.sharma22@delhi.gov.in** on or before date mentioned in fact sheet in the format given below-

S. No.	RFP Document Reference & Page Number	Content of RFP requiring Clarification(s)	Points of clarification
	Add rows as per your queries.		

DeGS shall not be responsible for ensuring that the bidders' queries have been received by them. Any requests for clarifications post the indicated date and time may not be entertained by the DEPARTMENT OF INFORMATION TECHNOLOGY, GNCTD.

Responses to Pre-Bid Queries and Issue of Corrigendum

- a) The Nodal Officer notified by the DeGS will endeavour to provide timely response to queries deemed to be responded in the context of the tender scope. However, DeGS makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does DeGS undertake to answer all the queries that have been posed by the bidders.
- b) At any time prior to the last date for receipt of bids, DeGS may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document by a corrigendum.
- c) The Corrigendum (if any) & clarifications to the queries from all bidders will be posted on the Portal of DeGS/IT Department
- d) Any such corrigendum shall be deemed to be incorporated into this RFP.
- e) In order to provide prospective Bidders reasonable time for taking the corrigendum into account, DeGS may, at its discretion, extend the last date for the receipt of Proposals.

2.5 Amendment of Bidding Documents

At any time before the deadline for submission of bids, the DeGS, GNCT of Delhi may, for any reason, whether at own initiative or in response to a clarification requested by a prospective Bidder, modify the bidding document by amendment. The amended bid document will be uploaded on the portal

Section 3: Instructions to Bidder (ITB)

3.1 Preparation of Bids

3.1.1 Language of Bid

The bid prepared by the Bidder, as well as all correspondence and documents relating to the bid exchanged by the Bidder and the DeGS, GNCT of Delhi shall be written in Hindi or English language only.

3.1.2 Pre-Qualification Proposal

Please note that no price schedule whatsoever should be indicated in the Pre-Qualification proposal and should only be quoted in the Financial Bid. Refer Appendix I for Pre-Qualification Criteria. Indication of financial quote other than Financial Bid will invite rejection of bid at that stage only.

3.1.3 Financial Bid

Content and format of Financial Bid along with Evaluation Criteria is available at Appendix II

3.1.4 Undertaking

An undertaking from the Bidder with regard to compliance of all the terms and conditions of RFP shall be submitted along with Bid Document as per format given in Form-3.

3.2 Quoting for Bid Prices

3.2.1 Prices in the Price Schedule

The Bidder shall quote price in clear terms. Break up should abide by the Format for Financial Bid described in Appendix II. The rates quoted should be inclusive of all taxes (except GST), duties, levies, cess, overheads and other charges etc. and inclusive of delivery services at DeGS, GNCT of Delhi's premises up to the satisfaction of client or client's representatives. The aggregated price should be quoted in words also. The Financial Bids should strictly conform to the format given in Appendix-II to enable evaluation/comparison of bids and special care must be taken to ensure that the bids having any hidden costs or conditional costs and not conforming to the format given in Appendix-II will be liable for straight rejection.

3.2.2 Fixed Price

Prices quoted by the Bidder shall be fixed and no variation will be allowed under any circumstances till the completion of the Project. The Bidder should provide a detailed cost breakdown for the project, including:

- Cost of security testing for 50+ applications
- Remediation support costs
- Any other relevant expenses (if applicable)

3.2.3 Bid Currencies

All Prices shall be quoted in Indian National Rupee (INR).

3.3. Bid Security

3.3.1. Amount of Bid Security

The Bidder shall furnish, as part of its bid, a bid security in the form of Demand Draft / Bankers' Cheque / Unconditional Bank Guarantee from **Scheduled Bank** drawn in favour of **Delhi e-Governance Society, GNCTD** of amount of **Rs. 2,00,000/- (Two lakhs only)** payable at Delhi. The bid security shall remain valid for 225 days from the date of the opening of bid. In exceptional circumstances the DeGS, Govt. of NCT of Delhi may solicit the bidder consent to an extension of the period of validity for further period.

The physical copy of bid security in form of Demand Draft / Bankers' Cheque / Unconditional Bank Guarantee shall be submitted at DeGS, 8th Level, B-wing, Delhi Secretariat, IP Estate, GNCTD on or before _____ time.

The scan copy of the bid security in the form of Demand Draft / Bankers' Cheque / Unconditional Bank Guarantee shall be mail/post/by hand to the DeGS office before the bid closing date.

3.3.2. Discharge of Security Bid of Unsuccessful Bidder

Bid Security of unsuccessful Bidders will be discharged / returned within 30 days after the award of contract to the successful bidder i.e. issue of Lol, pursuant to ITB Section 3.

3.4. Period of Validity of Bids

3.4.1. Validity Period

Bids shall remain valid for 180 days after the date of bid opening prescribed by the DeGS, GNCT of Delhi.

3.4.2. Extension of Period of Validity

In exceptional circumstances, the DeGS, GNCT of Delhi may solicit the Bidder's consent to an extension of the period of validity of Bid.

3.4.3. Submission of Bid

Bids "Bids must be submitted via email, post, or by hand only before the stipulated deadline. The Department/Service Provider will not be responsible for any delays caused due to any reason. Bids submitted via email must be in PDF format.

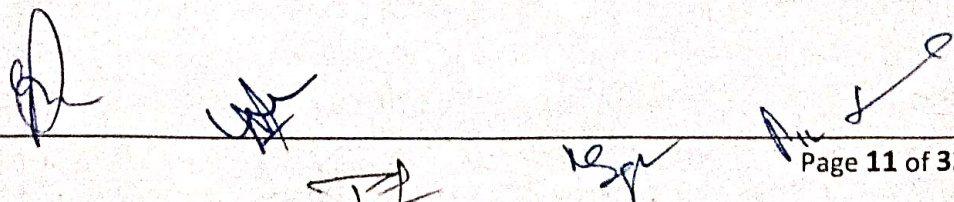
The following address should be used for submitting bids by post or by hand:

To
Member Secretary
Delhi e-Governance Society
Govt. of NCT of Delhi
Room No. 903, B Wing, Level 8
Delhi Secretariat, I.P. Estate
New Delhi - 110003".

3.4.4. Mailing Address for EMD of Bids

The following address should be used to submitting the EMD:

To



Member Secretary

Delhi e-Governance Society

Govt of NCT of Delhi, Room No. 903,

B Wing, Level 8, Delhi Secretariat,

I.P. Estate, New Delhi 110003

Marked as "Bid for Security Audit of IT Systems in GNCTD".

3.4.5. Rejection of Bid

If a bid is not responsive and does not fulfil all the conditions it will be rejected by the DeGS, GNCTD.

3.4.6. Extension for Last date for Submission

DeGS, GNCTD may, at his own discretion, extend the deadline for submission of bids by amending the bid documents in accordance with ITB Section 3, in which case all rights and obligations of the Client and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended. The extension of the deadline will be done only in exceptional cases.

In the event of specific date of submission of the bid/opening of the technical or financial bids being declared holiday for the client, the bid will be received/opened upto the appointed time on the next working date.

3.4.7. Bid Opening and Evaluation of Bids

a) Opening of Bids

The 'Pre-Qualification Bids' will be opened on the AFORESAID DATE in the office of Member Secretary, 9th Floor, B-wing, Delhi Secretariat, IP Estate, New Delhi in the presence of bidders or their authorized representatives who choose to attend.

b) Announcement of Pre-Qualification Bids

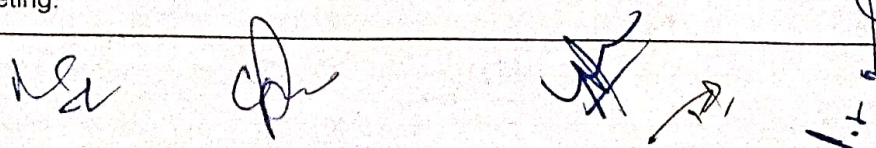
The Bidder's names, the presence or absence of requisite bid security will be announced by the client at the time of opening of bids.

c) Opening of Financial Bids

Only those Financial Bids will be opened and compared whose bids are technically qualified in the Pre-Qualification stage.

d) Announcement of Financial Bids

The Financial Bids will be opened, in the presence of Bidders' representatives who choose to attend the Financial Bid opening on date and time to be communicated to all the technically qualified Bidders. The name of Bidder, Bid Prices along with the financial components, etc. will be announced at the meeting.



3.4.8. Pre-qualification, Evaluation and Comparison of Bids

A two-stage procedure will be adopted for evaluation of proposals, with the Prequalification being completed before the financial proposals are opened and compared. The financial bids of only those bidders who qualifies all PQ criteria will only be considered for financial bid evaluation.

3.4.9. Contacting the Client

No Bidder shall contact the Client on any matter relating to its bid, from the time of the bid opening till the time the Contract is awarded. Any effort by a Bidder to influence the Client in his decisions on bid evaluation, bid comparison or contract award may result in rejection of the Bidder's bid.

3.5. Issue of Work Order & Signing of Contract

3.5.1. Client's right to accept any Bid and to reject any Bid or all Bids

The Client reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time before the contract is awarded, without thereby incurring any liability to the affected Bidder or Bidders.

3.5.2. Notification of Award (Letter of Intent (LOI))

Before the expiry of the period of validity of the proposal, the Client shall notify the successful Bidder in writing. The Lol shall be sent to the successful bidder through email provided in the bid document and the letter. The Bidder shall acknowledge in writing the receipt of the notification of award and will send his acceptance to enter into agreement within seven (7) days of issue of LOI. After receiving of written acceptance, the work order will be given to the vendor to execute the project.

3.5.3. Signing of agreement

The authorized signatory of DeGS shall sign an agreement with the successful Bidder on the terms and conditions decided mutually within the scope and purview of the RFP.

3.5.4. Expenses for the Contract

The incidental expenses of execution of agreement / contract shall be borne by the successful bidder.

3.5.5. Failure to abide by the Agreement

The conditions stipulated in the agreement shall be strictly adhered to and violation of any of the conditions will entail termination of the contract without prejudice to the rights of the DeGS with such penalties as specified in the Bidding document and the agreement.

3.5.6. Performance Guarantee

Period for Furnishing Performance Guarantee

Within seven (7) days of the issue of the work order the successful Bidder shall furnish the

performance guarantee of Rs.5,00,000/- (Rupees Five Lakh only), in the form of unconditional Bank Guarantee from **Scheduled Bank** or Demand Draft / Bankers' Cheque drawn in favour of "**Delhi e-Governance Society**" payable at Delhi. The validity of performance guarantee will be of 30 months from the date of issue of work order. This performance guarantee may be extended for another period of one year in case extension of one year be given to the bidder. The Bid security will be refunded once the Performance Bank Guarantee will be received from successful bidder.

3.5.7. Terms of Payment

- a) The payment to the Successful Bidder for this project will be done under the Annual Contract (Currently valid for two (2) years) on Quarterly basis.
- b) For release of these payments, the Successful Bidder shall present pre-receipted bills in triplicate (the bills shall be inclusive of all taxes, levies, duties, cess, overhead charges etc.) for the payments due to him along with all necessary supporting documents.
- c) For all the above tasks Successful Bidder will raise the bill after each quarter.
- d) The Delhi e-Governance Society will make effort for bill payment within 30 working days of submission of bill to the DeGS.
- e) In the event of termination of contract, the quantum of payment to be made to the Tenderer or the amount recoverable, as the case may be, shall be decided by the DeGS with regard to the work completed, expenditure incurred by the Tenderer (duly supported by adequate documents), payments already made by the Society etc. The decision of the DeGS in this regard shall be final and binding on both the parties i.e. the Successful Bidder and the DeGS.

3.5.8. No Claim Certificate

The Successful Bidder shall not, be entitled to make any claim, whatsoever, against the Client under or by virtue of or arising out of this contract nor shall the Client entertain or consider any such claim after Bidder shall have signed a "no claim" certificate in favour of the Client in such forms as shall be required by the Client after the works are finally accepted.

3.5.9. Termination

The contract will be terminated:

- 1) If the successful bidder fails to perform its obligations under the contract
- 2) In case of repeated failure in meeting the conditions of SLA

A 30 days notice will be issued to the bidder to rectify the shortcomings before the termination of the contract. In case successful bidder fails to rectify the shortcomings, the Client may, by a written notice of termination, terminate all payments to the qualified Bidder under the contract, which will further lead to termination of services of Bidder. If the qualified Bidder fails to perform any of its obligations under the contract, (including the carrying out of the services) provided that the such notice of termination:

- Shall specify the nature of the failure and
- Shall request the qualified Bidder to rectify such failure/defect within a specified period from

the date of issue of such notice of termination.

3.5.10. Standard of Performance

The qualified Bidder shall carry out the service and all the obligations under the contract with due diligence, efficiency and economy in accordance with generally accepted norms techniques and practices used in the industry. The qualified Bidder shall also employ appropriate / updated technology as well as safe and effective equipment, machinery, material and methods at its own cost.

3.5.11. Penalties

Delay in Deliverables

- a) 1% of Quarterly payment will be deducted for delay in deliverables for 1st week

2% of Quarterly payment will be deducted for delay in deliverables for 2nd week

3% of Quarterly payment will be deducted for delay in deliverables for 3rd week

4% of Quarterly payment will be deducted for delay in deliverables for 4th week

If it is delayed by 4 weeks, it means cumulative 10% of quarterly payment will be deducted.

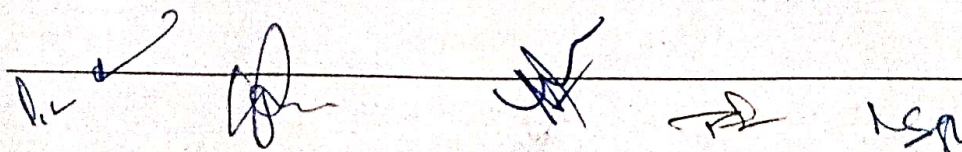
- b) Vulnerabilities once identified/fixed should not crop up again. If any of the already fixed vulnerabilities are reported by NIC/other external agencies, in that case a penalty of Rs.10,000/- will be imposed on the vendor.

Vulnerability once fixed on a page should **NOT** crop up again on the same page. To further secure an application, "No update should be done on application/server without a security Audit"

- c) After first cycle, if some vulnerability (s) are being identified/reported by any of the agencies viz CERT-IN, NIC etc, the vulnerabilities are to be fixed within 4 days time. Failing, penalty of Rs.1000/- per vulnerability incident shall be imposed on the vendor.
- d) If in case, penalty is imposed by invoking above mentioned a, b, c clauses, maximum penalty which can be imposed within a quarter year is 10% of quarterly payment.
- e) None of the resource person can be replaced before 6 months or completion of first cycle whichever is later from the start of the project. Thereafter, if needed maximum 2 resources can be replaced per annum with consultation of DeGS during the rest of the project. If the vendor still needs to replace more resources, a penalty of Rs.50,000/- will be charged per resource.

3.5.12. Force Majeure

- a) Notwithstanding the provisions of the tender, the Bidder shall not be liable for forfeiture of its performance guarantee, liquidated damages or termination for default, if and to the extent that, it's delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.
- b) For purposes of this Clause, "Force Majeure" means an event beyond the control of the Bidder and not involving the Bidder and not involving the Bidder's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Client either in its sovereign or contractual capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.



- c) If a Force Majeure situation arises, the qualified Bidder shall promptly notify the Client in writing of such conditions and the cause thereof. Unless otherwise directed by the Client in writing, the Bidder shall continue to perform its obligations under the contract as far as reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. The Client may terminate this contract, by giving a written notice of minimum 30 days to the Bidder, if as a result of Force Majeure, the Bidder being unable to perform a material portion of the services for a period of more than 60 days.

3.5.13. Arbitration and Jurisdiction

- a) If any dispute arises between the Parties hereto during the subsistence or thereafter, both Parties hereto shall endeavour to settle such dispute amicably. If attempt to bring an amicable settlement is failed, an arbitrator/arbitrators will be appointed by mutual consent. The Arbitration proceeding shall be governed by the Arbitration & Conciliation Act, 1996. The place of Arbitration shall be Delhi. The award given by the arbitrators will be binding on both the parties.
- b) The contract shall be interpreted in accordance with the Indian law/Contract Act.
- c) Place of Jurisdiction will be Delhi High Court.

3.5.14. Blacklisting

Company should not have been already blacklisted by the Government of India/UT or any other state of India. Bidder should therefore submit a self-attested Undertaking that their company has not been blacklisted by central or any state government.

The Department reserves the right to carry out the capability assessment of the "Bidder" and the Departments decision shall be final in this regard.

3.5.15 Contract Period

The period of the contract awarded to the bidder is 2 years. The contract period of project may be extended for an additional period of one year, subject to satisfactory services by the services provider and mutual agreement between both the parties. The terms and conditions agreed upon initially shall continue to apply during the extended period. However, final decision shall rest with the department.

3.6. Time line :

The timeline for submitting the security audit report for any website or application will be 10 working days from the date the request is formally communicated by the department.

Section 4 - Scope of work to be included

Scope of work defines the essential details of items/services required.

A rapid growth in discovered vulnerabilities in applications allows the HTTP/HTTPS and other protocols to become an attacker's easiest path into a network. In-house and commercially developed applications often put speedy development and convenience over security, which results in vulnerabilities such as Authentication bypass, SQL Injection, Cross site scripting etc. Applications are

also a preferred target for attackers, as they almost always allow access into internal resources through the firewall.

4.1. Suggestive Methodology for Vulnerability Assessment

4.1.1. Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls. A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human, or environmental. In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include "natural flood" because of the low likelihood of such an event occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or a benign, but nonetheless purposeful, attempt to circumvent system security.

4.1.2. Threat-Source Identification.

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat sources that are applicable to the IT system being evaluated. Threat-Source can be broadly classified as:-

- a) Intent and method targeted at the intentional exploitation of a vulnerability.
- b) A situation and method that may accidentally trigger vulnerability.

4.1.3. Vulnerability Identification

Vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. Table below presents examples of vulnerability/threat pairs. Methodology for security assessment should include, but not limited to, all the checks for the security issues as listed below:

- Broken Authentication
- Broken Access Controls
- Privilege elevation

- Forceful Browsing
- Broken Session Management
- Cross-site scripting
- SQL Injection
- Other injection flaws
- Cookie Poisoning
- Denial-of-service (DOS)
- Directory traversal
- Parameter tampering
- Weak Cryptography
- Improper Error Handling
- Third Party Misconfigurations
- Information leakage

Typical vulnerabilities that could be identified, but not limited to, during the assessment are as follows:

- Cross-site scripting
- SQL injection
- Server misconfigurations
- Form/hidden field manipulation
- Command injection
- Cookie poisoning
- Well-known platform vulnerabilities
- Insecure use of cryptography
- Back doors and debug options
- Errors triggering sensitive information leak
- Weak passwords
- Weak session management
- Buffer overflows

- Forceful browsing
- CGI-BIN manipulation
- Risk reduction to zero day exploits

Vendor's application security audit should provide a standard audit report and audit checklist on the effectiveness of the security controls that exist in Departments/Local bodies/Corporations under Government of NCT of Delhi as per report format in Annexure V. The report should also provide remediation advice for those items discovered along with a detailed explanation followed by fixing of the vulnerabilities reported. Once the vulnerabilities are fixed, a follow-up test should be carried out to ensure that all the vulnerabilities originally found are fixed.

4.1.4. Penetration Testing (PT)

New threats are evolving day-by-day with the evolving technology and hence organizations face challenges to maintain security if their information security assets. Often organizations leverage new technologies to extend their functionality and reach more clients and partners and hence their exposure to risk grows continuously. Insecurely deployed networks, hosts, and applications are common attack surfaces for hackers to exploit and resulting in loss of confidentiality, integrity, or availability of the information system assets.

Vendor must ensure that penetration testing service that they provide attempts to simulate the techniques adopted by an attacker to compromise Delhi government websites information systems. It should highlight critical vulnerabilities which could be exploited by an attacker to compromise various information systems.

The Penetration testing must include the following but not limiting to :-

- a) Remotely audit and analysis of security loopholes, if any, on the given IP address. Try and exploit the vulnerabilities detected.
- b) Analyze the services running on the servers and the firewall policy for any security lapses. Hardening of servers and networking as per existing policies in force.
- c) Automated attempt to guess passwords using password-cracking tools.
- d) Search for back door traps in the programs.
- e) Attempt to overload the system using DDOS (Distributed Denial of Services) and DoS (Denial of Services) attacks.
- f) Checking if commonly known holes in the software, especially the browser and the e-mail software exist.
- g) Checking for the other common vulnerabilities like IP Spoofing, Buffer overflows, Session hijacks, Account spoofing, Frame spoofing, caching of web pages, cross-site scripting, Cookie handling etc.
- h) Prepare an Executive Summary as well as a Detailed Technical Report on the findings together with recommendations.

4.1.5 Network Audit

The vendor will perform the network audit of the departments as and when it is required by the DeGS.

4.1.6 Mobile App Audit

The vendor will perform the mobile applications audit for all types of mobile. It includes corresponding APIs and UI of the system

4.1.7. STQC GIGW compliance

STQC GIGW compliance audit for the website/portal to be carried out by the agency whenever required.

4.2. Responsibility of the Bidder

The firms are required to undertake the correct course of action to identify vulnerabilities. The firm shall follow standard procedures of security audit and guidelines/ advices in Information Security Policy / CERT-IN

4.2.1. Responsibilities

The bidder will be responsible for the following:

- a) The bidder will be responsible to provide Five (5) Resident Engineers (as mentioned in section 4.2.2) to conduct the Vulnerability Assessment for Applications/Software running in various department of GNCTD. With due course, if a need arises to have more resident engineers, DeGS GNCTD may hire them as per the rates finalized during this bidding process and it will be binding on successful bidder to provide the same.
- b) For the applications built by NIC or any other external vendors, bidder will also be responsible for guiding and recommending technical/process steps to 'how to fix' certain vulnerabilities.
- c) CERT-IN Security and Quality standards to be followed as listed on www.cert-in.org.in/
- d) STQC – Security guidelines as mentioned at <http://www.stqc.gov.in>
- e) To check if all the standards/Guidelines for Indian Government Websites issued by NIC are being followed.
- f) The standard assessment / audit report(s) should identify and prioritize risks based on severity correlating the same with industry standards and client business requirements.
- g) Periodic scheduled assessments should be treated as the essential component in Information Security program for all Web Applications and portals running in Delhi Government.
- h) Tests must be followed up by diligent closure of all identified threats and vulnerabilities.
- i) Post remediation, a second assessment or subsequent retests must be carried out in a similar way to ensure all identified gaps are closed and that the remediation exercise has not resulted in any new weaknesses. A timeline of 07 working days shall be given for retest and submission of retest audit report along with recommendations steps for vulnerabilities fixing.
- j) Security Audit Certificate / Security Audit Compliance Report must be issued per application.

Man power on the Project

The vendor should provide 05 Highly Qualified and Experienced Resident Engineers who will perform the Security Audit of all the IT Systems running in Delhi Government on regular basis. The resident engineers MUST have extensive experience in security assessments and hold at least one of the internationally recognized professional certifications such as CISA (Certified Information Systems

Auditor), CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker).
The desired qualification, skill set and experience for required professionals is as :-

Designation	No. of Persons	Qualification	Certifications	Experience
Senior Resident Engineer	2	B.E/B.Tech/M.E/ M.Tech/MCA from recognized Institutions as per UGC/AICTE	CISA/ CISSP/ CEH/OSCP	8 yrs with min 4yrs in Security Audit/Cyber Security/mobile security testing(iOS & Android)
Junior Resident Engineer	3	B.E/B.Tech/M.E/ M.Tech/MCA from recognized Institute as per UGC/AICTE	CISA/ CISSP/ CEH/GIAC/ GWAPT	4 yrs with min 2 yrs in Security Audit/Cyber Security

In addition to above, the resident engineers must have working knowledge of SQL server, database design and development, covering constraints, indexes, views, functions, stored procedures, joins, cursors and triggers etc. With due course, if the need arise to have more resident engineers, DeGS GNCTD may hire them as per the rates finalized during this bidding process. The task to be performed are listed as above:

- Oversee all testing activities
- Validate the results of vulnerability assessments
- Provide guidance on remediation and consult with the Client's technical teams
- Perform detailed web application security assessments, focusing on OWASP Top 10 vulnerabilities
- Conduct penetration tests for authentication, session management, and business logic flaws
- Generate reports and recommendations based on findings
- Perform static and dynamic security analysis of mobile apps
- Assess platform-specific vulnerabilities and weaknesses in mobile app architectures
- Conduct network security tests and analysis of app-data communication
- Conduct automated vulnerability scans on all applications
- Interpret scan results, prioritize risks, and work with remediation teams
- Track and manage vulnerabilities from identification to resolution
- Provide recommendations for secure coding practices to prevent future vulnerabilities

In case, the current deployed Resident Engineer moves out of the project – only a higher qualified or equally qualified engineer with same experience should replace him only in consultation with Delhi e-Governance Society.

4.2.2. Standard Activities to be performed

Following Standard Activities should be performed by Resident Engineers :

1. Security Audit of all IT/Web/Mobile enabled Applications
2. Each application should be Audited quarterly.
3. Audit Certificate to be issued for each application.
4. Submit the vulnerability report in CERT-In prescribed format (Refer to Annexure 'V') for each vulnerability found in the application.

5. It should be noted that out of all the applications, some of the applications were built by external agencies through Tendering process and they might be in support phase. For such applications the vulnerability report should be submitted to the respective department for that application who will further get those vulnerabilities removed from the system.
6. Access to deployed application, access to source code and fixing rights will be provided by concerned departments.
7. Periodic Progress & performance report should be submitted to DeGS, GNCTD.

4.2.3 Applications to be Tested

The Bidder will conduct security testing on a total of 50+ web and mobile applications, encompassing a variety of platforms and frameworks (e.g., iOS, Android, various web frameworks).

4.2.4 Security Testing Types

The Bidder must perform the following types of security tests:

Web Application Security Testing

- OWASP Top 10 Testing
- Authentication & Authorization Testing
- Business Logic Testing
- Data Validation Testing
- Vulnerability Scanning (SQL Injection, Cross-Site Scripting, etc.)

Mobile Application Security Testing

- Static & Dynamic Analysis
- Network Security Testing
- Code Review
- Platform-Specific Security Tests

The Bidder must employ industry-standard security testing tools and techniques to ensure comprehensive coverage and accuracy of results. Tools may include but are not limited to:

- Burp Suite, OWASP ZAP (for web app testing)
- Mobile Security Framework (MobSF)
- Nessus, Qualys, or OpenVAS for vulnerability scanning

4.3. Documentation

The firm should prepare documentation for each Security Audit as per the guidelines brought out below:-

Audit Report. Audit reports are crucial documents. The formal IT security audit report is a key audit output and must contain the following:-

- Identification of auditee (Address & contact information).
- Dates and Location(s) of audit.

- Terms of reference (as agreed between the auditee and auditor), including the standard for audit.
- Audit plan.
- Explicit reference to key auditee organization documents (by date or version) including policy and procedure documents.
- Additional mandatory or voluntary standards or regulations applicable to the auditee.
- Summary of audit findings including identification tests, tools used and results of tests performed.
- Analysis of vulnerabilities and issues of concern.
- Recommendations for action.
- Others (will be decided on need basis)

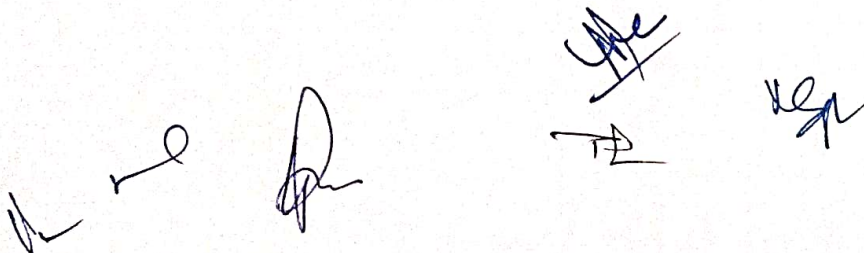
4.3.1 Initial Assessment Report: A detailed report outlining the vulnerabilities discovered, categorized by severity (e.g., Critical, High, Medium, Low).

Final Report: After the vulnerabilities have been addressed, a comprehensive report including fixed issues and validation of resolutions.

- **Support Services:** The Bidder should provide consultation and support for fixing reported issues. This includes assisting the development team in understanding and resolving the vulnerabilities.

Apart from above, the resident engineers will plan proper reporting mechanism in consultation with DeGS including various reports like Vulnerability Report, Incident Report, Guidelines compliance report etc.

No penalty shall be levied for delay attributable to DeGS, GNCTD, or in case of Force majeure events

The block contains five handwritten signatures or initials in blue ink. From left to right: a stylized 'H' or 'M', a signature with a long horizontal stroke, a signature with a large loop, a signature with a cross-like mark, and a signature with a large 'K' or 'R'.

Appendix 1: Pre-qualification Criteria

The Bidding is open to all qualified Bidder who fully meets the following qualifying requirements:

S No	Pre-Qualification	Required Document
1	The word "Company" / "Audit Agency" here includes registered company under Indian Companies Act, 1956. The company should be 10 (Ten) years old.	Certificate of Incorporation and Articles & Memorandum of Association of the bidder.
2	The average turnover of "Company" for the last three years should not be less than Rs 5,00,00,000/- Five crores from all services and minimum of Rs.2,50,00,000/- (Two crores and Fifty Lacs in area of Security Audit of IT Systems. The Bidder should have been making profits in the last three financial years	CA Certificate to be attached The Balance Sheet of the company of the last three years
3	The "Bidder" should have its registered or branch offices in the Delhi NCR region at the time of submission of bid.	Proof of address
4	The Bidder should commit to deploy at-least 5 Resident Engineers (2 senior and 3 junior engineers) in the project possessing relevant experience in similar field as mentioned in Section 4.2.2 of bid document	Yes/No Undertaking on company letter head and Attested.
5	Company has not been blacklisted by the Government of India/UT or any other State of India	Attach undertaking
6	Whether in last 5 (Five) years , the company has experience in the Govt./PSU/Autonomous bodies i) For providing Security Auditing manpower for websites/ Portals/ IT Systems for 1 work orders of Security audit of at least value of Rs. 80,00,000/- or ii) For providing Security Auditing manpower for websites/ Portals/ IT Systems for 2 work orders of Security audit of at least value of Rs. 50,00,000/- or iii) For providing Security Auditing manpower for websites/ Portals/ IT Systems for 3 work orders of Security audit of at least value of Rs. 40,00,000/- The Work order should not be issued more than five year as on last date of bid submission.	Copy of the Work order and completion certificate from the respective client.
7	The firm/company should have 50 qualified personnel in the areas of IT security audit who possess prior experience of at least 5 years as on date in providing IT Security Auditing services.	Letter from authorized signatory and also copy of Professional certificates from certified agencies like (CISA/ CISSP/ CEH/OSCP/ GIAC/GWAPT)
8	Attached the following copies of the valid A. PAN No. b. GST Registration No.	Yes/No Copies of all mentioned documents

9	Latest valid ISO 9001:2008 and ISO 27001 (attach certificate) or higher	Yes/No Copy of ISO certificate
10	The bidder should be CERT-In empanelled security auditing organization/agency continuously for the last ten (10) years and must hold a valid empanelment for the next two (2) years.	Copy of Cert-In empanelment letter
11	Scan copy of EMD, in addition to physical submission, to be attached online or relevant certificate for EMD Exemption to be attached	Copy of EMD or copy of certificate for EMD exemption
12	Form A, B and C as attached in RFP	Attached Signed Copy.

Note: Financial evaluation of only those vendors will be carried out, who fulfils all the conditions of the Pre-Qualification Criteria as mentioned above. The Bids which could not fulfil the Pre-Qualification Criteria shall be rejected. The Master Service Agreement (MSA) will be signed with the L1 bidder once they have been finalized. This agreement will outline the terms and conditions of the project, including the scope of work, deliverables, timelines, and payment terms, ensuring a formal and legally binding arrangement between the two parties.

Form A: Bid Application Sheet

Name of the Company	
---------------------	--

Registered Office Address		
No.		
Street		
Area/ Locality		
City		Pin -
Telephone		Fax -
Email		
URL		
Local Office Address :		
No.		
Street		
Area/ Locality		
City		Pin -
Telephone		Fax -
Email		
Contact Person		
Name		
Designation		
Telephone		Fax
Email		

Form B: Undertaking

1. It is certified that the information furnished here in and as per the document submitted is true and correct and nothing has been concealed or tampered with. We have gone through all the conditions of RFP and are liable to any punitive action for furnishing false information / documents.
2. The technical solution offered fully meets your requirements and have no deviations and variations to the scope of work defined in this RFP. The entire work shall be performed as per DoIT, GNCT Delhi's specifications and documents.
3. I will not change any amount for any additional or new tools/software needed for delivery of work/service as part of scope of work awarded.

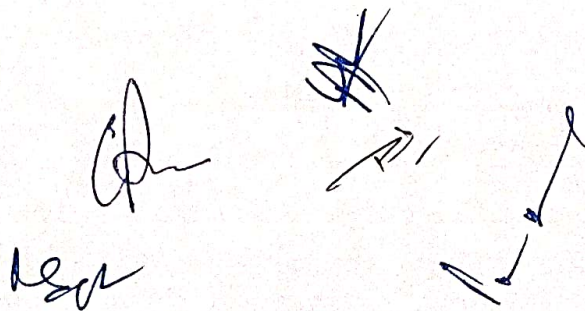
Dated this _____ day of _____ 202__

Signature

(Company Seal)

_____ In the capacity of

Duly authorized to sign Applications for and on behalf of:



Form C: Warranty

(Please see Section 3 for the General Conditions of Contract)

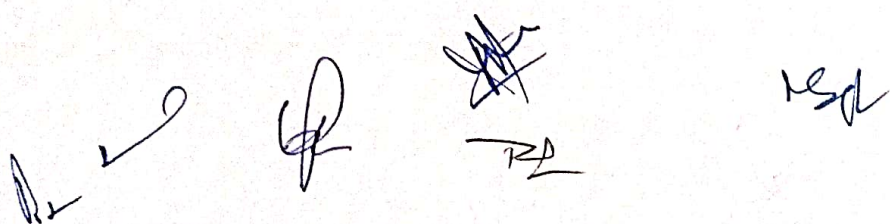
WARRANTY

We warrant that all Security Auditing processes and therefore the vulnerability fixing suggestions shall be based on most recent and current techniques. We shall be fully responsible for vulnerability reporting of all the applications and ensuring that they are fixed by respective departments in best possible manner.

The Warranty will be valid for 18 months from the date of (process here). The obligation under warranty shall include all costs relating to Security Auditing as well as vulnerability fixing suggestions of all the Application Software running under the scope of this Contract,

Signature of the Witness

Signature of the Tenderer

The block contains four handwritten signatures. The first two are on the left, under the 'Signature of the Witness' line. The next two are on the right, under the 'Signature of the Tenderer' line. The signatures are in blue ink and vary in style, with some being more stylized or crossed out.

Appendix II: Content and Format of Financial Bid

Sr. No.	Resource Type	Qty.	Rate per unit Per month(including all taxes) except service tax/GST	Total
1	Senior Resident Engineer	2		
2	Junior Resident Engineer	3		
			Grand Total	
Grand Total (In words)				

L1 bidder will be decided on the lowest value of Grand Total

Rate of other resources, institutional cost & deployed Hardware/software etc., are part of final cost. I am as bidder understand that no additional cost will be payable to be for institutional /organisational knowledge, support and establishment of Assessment Lab

(Sign and Stamp of Authorized Person)

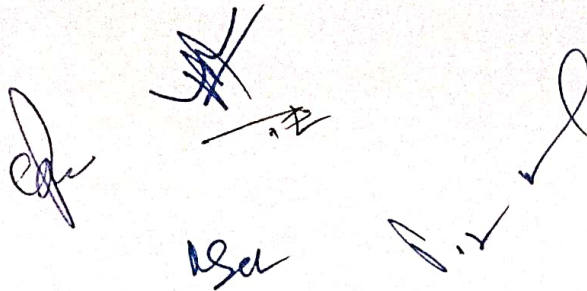
Appendix III: List of Applications to be Audited/rectified

It is advised to Bidder that they should go to GNCTD website www.delhi.gov.in which is a composite website of all departments under GNCTD and links to various operational applications are available there.

Indicative list of Applications:

1. https://testepds.delhigovt.nic.in/FCI_WR/Login.aspx
2. <https://ceodelhinet.nic.in/OnlineErmsDept/Login.aspx>
3. <https://covidldelhi.nic.in/>
4. <http://auth2.dusibrehab.in/>
5. <https://stagingdlsc.delhi.gov.in/IFMSDJBPORTAL>
6. <https://audit-delhi.aksamity.com/>
7. <http://15.207.107.166/>
8. <https://testserver.delhigovt.nic.in>
9. 10.128.88.67:8080/agriculture
10. <https://stagingdlsc.delhi.gov.in/payrollaudit/login.aspx>
11. stagdsssonline.nic.in
12. <https://stagingdlsc.delhi.gov.in/gpf/login.aspx>
13. stagingtradsssb.nic.in
14. <http://10.128.30.41>
15. <http://srams.delhi.gov.in/rarstest11>
16. 10.128.119.22
17. aaagh.delhi.gov.in
18. <http://10.194.163.238/>
19. <http://10.194.163.238>
20. <http://10.247.206.189:82/>
21. gsdlapp02.org.in/pdm_sop_final
22. <https://djbstaging.watsoo.com/>
23. <https://10.128.119.27/>
24. <https://www.ceodelhi.gov.in/>
25. 164.100.72.248
26. Electoral Literacy Club ELC App
27. Delhi Election
28. CEO Delhi Officers portal
29. <http://gsdlapp02.org.in/DJB/login.php>
30. gsdlapp02.org.in/revenue
31. gsdlapp02.org.in
32. gsdlapp02.org.in/hfw2/
33. <http://gsdlapp02.org.in/fivejidata/>
34. gsdlapp02.org.in/easeofdoing/
35. <http://gsdlapp02.org.in/5grollout>

- 36. [://164.100.190.83](http://164.100.190.83)
- 37. <http://10.128.30.7>
- 38. <https://stagingdlsc.delhi.gov.in/Gst/Account/Login.aspx>
- 39. <https://stagingdlsc.delhi.gov.in/elekha/login.aspx>

The image shows four handwritten marks in blue ink. On the left is a cursive signature. In the center is a signature with a large 'X' over it. Below the central signature are the initials 'HSC'. To the right is a signature that appears to be 'P. V.' followed by a large loop.

Appendix IV : CERT –IN Format of reporting Vulnerability (Indicative)

For official use only: Vulnerability number #		
1. Contact Information of the person reporting:		
Name:	Organization:	Title:
Office Phone:	Email:	Fax Number:
Cell Phone/ Pager:		
Address:		
2. Date and Time of Identification:		
Date:	Time:	
3. Type of Vulnerability (check all that apply):		
Input Validation error	Environment Error	
Boundary Condition error	Configuration Error	
Buffer Over Flow	Race Condition	
Access Validation Error	Others	
Exceptional Conditional Error		
4. Common Weakness Enumeration (CWE) : (if any)		
5. Information of Affected System:		
Application	Operating System	Hardware
Name	Name	
Version	Version	
Release	Release	
6. Vulnerability Description (Attach additional sheets if required):		
7. Vulnerability Consequences:		

8. Suggested Solution:
9. Other Agencies Notified:
10. Additional Information:

Note 1: The Technical Bid must include the following:

- Proposed Methodology for execution
- Proposed Plan
- Security Architecture Design
- Details of Hardware and software to be used
- Project Plan
- Vulnerability Assessment plan

