File No. xx(xx)/2025-NIC

एनआईसी
National
Informatics
Centre

NATIONAL INFORMATICS CENTRE

Request For Proposal (RFP)

for

Selection of Managed Service Provider

for Supply, Operations and Management of ZTNA Solution/Licenses

Bid Number GeM/2025

Address: National Informatics Centre, A-Block, CGO Complex

New Delhi-110003

Phone:

Email:

Table of Contents

1 Definitions & Abbreviations

1.1 Definitions

1.1.1In this bid document, the expressions in column (2) in Table 1 shall have the meanings respectively assigned to them in the corresponding entry in column (3).

TABLE 1: DEFINITIONS

S. No.	Expression	Definitions
1.	Annual	A period of 12 Months, reckoned from the date of issuance of Work Order and, in respect of any period constituting less than a period of 12 Months in the period preceding the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, such lesser period.
2.	Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
3.	Auditor	The Statutory Auditor of a company/ Bidder/MSP
4.	Authorised Representative	For the doing of any act or thing, for the purposes of the bid or identification of the Selected MSP or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected MSP or Purchaser, as the case may be, may specify as its Authorised Representative in this behalf.
5.	Authorised Signatory	For the affixation of signature or Electronic Signature Certificate on any Document or electronic record, for the purposes of the bid or identification of the Selected MSP or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected MSP or Purchaser, as the case may be, may specify as its Authorised Signatory in this behalf.
6.	Bid	The bidding process and the proposal submitted by the Bidder for this bid, including any clarifications and amendments by the Bidder in response to any request made by the Purchaser in this connection.
7.	Bidder	The organisation participating in the Bid process, pursuant to this bid.
8.	Managed Service Provider (MSP)	The MSP with whom the Purchaser enters into the Contract (Selected /Successful Bidder).
9.	Client	Shall mean the Organisations for which order(s) will be issued.
10.	Commissioning	The final process of ensuring that the equipment or system is fully operational, integrated, and ready for its intended use.

11.	Confidential Information	Any information disclosed to or by any Party to this Contract and includes any information in relation to the Parties, a third party or any information including any such information that may come to the knowledge of the Parties hereto / Service Provider by virtue of this Contract that is by its nature confidential or by the circumstances in which it is disclosed confidential; or is designated by the disclosing Party as confidential or identified in terms connoting its confidentiality; but does not include information which is or becomes public knowledge other than by a breach of this.
12.	Contract Period	The period of subsistence of the Contract.
13.	Contract Value	“Contract Value” means 3 years value of BoQ as quoted in the commercial bid. The calculation shall be done assuming the BoQ and value remain same over the Contract duration.
14.	Contract/Agreement	The Contract or Agreement entered into between the MSP and the Purchaser.
15.	Day	Day means both working as well as non-working day, unless specified otherwise
16.	Document	Any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes or and databases or microfilm or computer-generated micro fiche.
17.	Endpoint	Standalone computers and computer resources connected to a network, restricted to desktops and laptops. For the purposes of this document, reference to ‘computer’ and ‘computer resource’ shall be construed as defined under the Information Technology Act, 2000 and shall specifically include only desktops and laptops mapped to endpoint security agents.
18.	Financial Year	The period from the first of April till the thirty-first of March of the succeeding calendar year.
19.	Go-Live	Refers to the Go-Live of ZTNA and commencement of operations.
20.	Implementation phase	The phase of the project before Go-Live
21.	Incident	Any unplanned interruption, degradation, or reduction in the quality of a service, or a failure of a component that has not yet impacted the service but has the potential to cause disruption. Incidents include, but are not limited to: • Unavailability or malfunction of systems, applications, or infrastructure. • Deviation from agreed Service Levels that impacts business operations. • Any event reported by users, or service staff which requires investigation and resolution to restore normal service.

22.	Month	A calendar Month of the Gregorian calendar and, in respect of any period constituting part of a calendar month— (a) in which the relevant contract was issued; or (b) which preceded the expiry of the period specified in the Contract period, whichever is earlier, such part of a calendar month; and the expression "Monthly" shall be construed accordingly.
23.	Net worth (Consolidated)	The aggregate value of the paid-up share capital and all reserves created out of the profits (Securities Premium Account and debit or credit balance of Profit and Loss Account), after deducting the aggregate value of the accumulated losses, deferred expenditure and miscellaneous expenditure not written off, as per the audited balance sheet as defined in Indian companies act 2013.
24.	On-premises/ on Prem	Software's, platform and components that are implemented on Bidder's supplied hardware in Purchaser's data centres through trust brokering/ authentication so that sensitive authentication data and processes remain within the organisation's-controlled environment.
25.	Operational phase	The phase of the project after Go-Live
26.	Party	Includes the Bidder and the Purchaser, and the expression "Parties" shall be construed as a reference to the two taken together
27.	Purchaser	NIC, including any— (a) of its successors. (b) representative authorised by it; and (c) assignee permitted by it
28.	Quarter	"Quarter" means a period of three Months, reckoned from the date of Go-Live and, in respect of any period comprising less than a period of three Months in the period preceding the termination of the Contract or the end of the Contract Period (including any period for which the Contract is extended), shall include such period, and the expression "Quarterly" shall be construed accordingly.
29.	Services	Services to be provided by the bidder for the discharge of its obligations under the bid document and the Contract, in a manner consistent with— (a) Applicable Law; and (b) extant policies and guidelines for— (i) cybersecurity, information security and data protection procedures and practices; and (ii) prevention, response and reporting of cyber

		incidents, issued by the Government of India, the Purchaser, the Indian Computer Emergency Response Team (CERT-In) in the performance of functions entrusted to it by law, or the National Critical Information Infrastructure Protection Centre (NCIIPC) in respect of such Critical Information Infrastructure as may be declared as a protected system by law, including such amendments or modifications thereto as may be made from time to time.
30.	Service Downtime	Non-availability of the ZTNA solution
31.	Single Point of Contact (SPOC)	Shall mean the designated person of the Purchaser.
32.	System/ICT	Includes but not limited to Applications/ Portals/ Cyber Security devices / Active Network Components/ End Points etc. The words have been used interchangeably.
33.	Technical Manpower/Resource	Technical manpower refers to a specialized workforce possessing the specific skills, knowledge, and expertise required to perform technical tasks. They should hold technical degree recognised by any government institution in India
34.	Turnover	The aggregate value of the realisation of amount made from the sale, supply or distribution of goods or on account of services rendered, or both, by a company during a financial year as defined in Indian companies act 2013 and its revisions.
35.	Total Quarterly payment	Total Payment to be made to the bidder against invoices submitted quarterly.
36.	Users	Administrator/ Application owner of an organisation.
37.	UAT	The process of testing of the complete solution made by the MSP for final acceptance of the Purchaser as per terms and conditions laid out in this bid document.
38.	User Organisations/ Organisations	One or more entities to which NIC provides information and communication technology (ICT) services or support, including— (a) a ministry, department, secretariat or office of the Central Government specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, and any other entity under the administrative purview of any such ministry, department, secretariat or office. (b) secretariats or offices of Lok Sabha, Rajya Sabha, Supreme Court of India, Delhi High Court and other NIC-supported Constitutional body or national level statutory body.

39.	Week	A period of seven consecutive days and, where the period to be reckoned in terms of weeks includes any part of a week, includes such part of a week.
40.	Work Order	An order placed by the Purchaser on the Managed Service Provider for providing the solution under the Contract for such period as may be specified therein or till the expiry of the Contract period, whichever is earlier.
41.	Working Day	Any day of the Week and does not exclude Sunday, or a Holiday declared by Purchaser and/or Government of India.
42.	ZTNA	A technology or service that provides secure remote access to an Organisation's applications and services based on clearly defined access control policies.

1.2 Abbreviations

TABLE 2: ABBREVIATIONS

S. No.	Abbreviation	Full Form/Definitions
1.	AMC	Annual Maintenance Contract
2.	API	Application Programming Interface
3.	AV	Anti-Virus
4.	BG	Bank Guarantee
5.	BoQ	Bills of Quantities
6.	CA	Chartered Accountant
7.	CERT-IN	Indian Computer Emergency Response Team
8.	CIN	Corporate Identification Number
9.	CPP	Central Public Procurement
10.	CSP	Cloud Service Provider
11.	CV	Curriculum Vitae
12.	DB	Database
13.	DC	Data Centre
14.	DCIM	Data Centre Infrastructure Management
15.	DNS	Domain Name System
16.	DR	Data Recovery
17.	ECS	Electronic Clearance Service
18.	EDR	Endpoint Detection and Response
19.	EMD	Earnest Money Deposit
20.	EPP	Endpoint Protection Platform
21.	FEC	Financial Evaluation Committee
22.	FIM	File Integrity Monitoring
23.	FS	Final Score
24.	GCC	Government Community Cloud
25.	GeM	Government e-Market Place
26.	GFR	General Financials Rules
27.	GoI/ GI	Government of India
28.	GST	Goods and Service Tax
29.	GUI	Graphical User Interface
30.	HDD	Hard Disk Drives
31.	HIPS	Host Intrusion Prevention System
32.	HQ	Head Quarters
33.	HSM	Hardware Security Module
34.	HTTPS	Hypertext Transfer Protocol Secure
35.	IaaS	Infrastructure as a Service
36.	IAM	Identity and Access Management
37.	ICT	Information and Communication Technology
38.	INR	Indian Rupees
39.	IOA	Indicators of Attacks

40.	IOC	Indicators of Compromises
41.	IP	Internet Protocol
42.	IPR	Intellectual Proprietary Rights
43.	ISO	International Organisation for Standardization
44.	IT	Information Technology
45.	ITB	Instruction To BIDDER
46.	ITeS	Information Technology Enabled Services
47.	ITSM	Information Technology Service Management
48.	KPI	Key Performance Indicator
49.	LAN	Local Area Network
50.	LCD	Liquid-Crystal Display
51.	LD	Liquidated Damage
52.	LoI	Letter of Intent
53.	MeitY	Ministry of Electronics & Information Technology
54.	MFA	Multi-Factor Authentication
55.	MPLS	Multi-Protocol Label Switching
56.	MSP	Managed Service Provider
57.	NAC	Network Access Control
58.	NAT	Network Address Translation
59.	NDC	National Data Center
60.	NEFT	National Electronic Funds Transfer
61.	NFS	Network File System
62.	NIC	National Informatics Centre
63.	NICNET	National Informatics Centre Network
64.	NIPS	Network Intrusion Prevention System
65.	NIT	Notice Inviting Tender
66.	NKN	National Knowledge Network
67.	NOC	Network Operations Centre
68.	NTP	Network Time Protocol
69.	OLE	Object Linking & Embedding
70.	OS	Operating System
71.	PaaS	Platform as a Service
72.	PAN	Permanent Account Number
73.	PBG	Performance Bank Guarantee
74.	PC	Personal Computer
75.	PoC	Proof of Concept
76.	PSU	Public Sector Undertaking
77.	RAM	Random Access Memory
78.	RAR	Roshal Archive format
79.	RFP	Request for Proposal
80.	RPO	Recovery Point Objective
81.	RTI	Right to Information Act
82.	RTO	Recovery Time Objective

83.	SaaS	Software as a Service
84.	SIEM	Security Information and Event Management
85.	SLA	Service Level Agreement
86.	SOC	Security Operations Centre
87.	SQL	Structured Query Language
88.	SSD	Solid State Drives
89.	SSO	Single Sign-On
90.	STQC	Standardization Testing and Quality Certification
91.	TCP	Transmission Control Protocol
92.	TCV	Total Contract Value
93.	TEC	Technical Evaluation Committee
94.	UAT	User Acceptance Test
95.	UEM	Unified Endpoint Management
96.	VM	Virtual Machine
97.	VPN	Virtual Private Network
98.	WAF	Web Application Firewall
99.	WAN	Wide Area Network
100	ZTNA	Zero Trust Network Access

2. Scope of Work

2.1. Through this bid, Purchaser envisages to select a Managed Service Provider who will supply, install, implement, support, maintain and operate, the Zero Trust Network Access (ZTNA) licenses/solution for endpoints deployed across Ministries/Departments/User Organisations for a period of three years (extendable up to two years based on mutual agreement between MSP and NIC) as per the T&Cs given in the bid document. That solution must enable secure application access by ensuring seamless, connectivity across all the endpoints in Government Departments/Ministries. The selected MSP shall be responsible for implementation and managing day to day operations of the solution throughout the Contract Period as mentioned in the bid Document.

2.2. The selected MSP shall ensure the seamless integration of the provided ZTNA licenses to fully utilize the security benefits they offer.

2.3. The Licenses procured as part of this Bid will be used for securing services under Zero Trust Network Access (ZTNA) for continued protection of critical infrastructure through secure, policy-driven access management and enforcement of least-privilege principles.

2.4. The selected MSP must also get the security audit by Cert-In empanelled auditor as per the scope of work and periodicity given in the bid document. The selected MSP shall integrate all the systems/components in the proposed solution with the current cyber security and IT operation systems of the Purchaser that include but not limited to Ticketing Platform, SOC, SIEM, SOAR, SSO, PIMS, ITAM, NTP, LDAP, AAA, Email, SMS gateway, Web Proxy etc. and all other cyber security and operations management systems which will be deployed from time to time.

2.5. The selected MSP shall ensure that all components (e.g. Hardware, software, etc) of the solution is free from any malicious code, hidden threats, or vulnerabilities that could compromise the Integrity, Confidentiality and Availability of Government data and systems.

2.6. In the event of non-compliance or detection of any malicious component at any stage, the MSP shall cooperate fully with NIC to investigate and remediate the issue. Consequences of such incidents, if any, shall be determined based on the nature and severity of the issue and in accordance with due process, which may lead to disqualification including blacklisting, and/or legal action as deemed appropriate by NIC.

2.7. Remote troubleshooting sessions will not be provided to the MSP/OEM due to the critical nature of the system.

2.8. The supplied Hardware and Software used for hosting ZTNA Solution must be capable of scaling to accommodate up to 25% of additional licenses.

2.9. Sub-contracting is strictly prohibited at any stage of the execution of this bid, except for the CERT-In empanelled auditor, who will be responsible for conducting the security audit under section 4.7, ‘Audit’.

2.10. The quantity of required licenses is defined in table 3 during the Contract period.

TABLE 3: BoQ

S. No.	Solution	Estimated Licenses in Quantity
1	Zero Trust Network Access (ZTNA)	3,00,000

Note: The Purchaser reserves the right to procure any quantity as deemed appropriate in single or multiple orders from the Bill of Material quoted by the Bidder during the contract period.

2.11. All the supplied components including Hardware, Software and OS shall be provided with full feature and functionality, without any licensing restrictions/limitations.

2.12. On-premises solution is required to be scalable, incorporating a minimum redundancy configuration of N+1. This design ensures that the system can maintain full operational functionality even in the event of a component failure, thereby enhancing reliability and performance.

2.13. The Bidder has to setup complete infrastructure On-premises (MSP’s supplied hardware in Purchaser’s Data Centre) as a managed service model (DC and DR).

2.14. Must have an intuitive graphical User Interface (GUI) for Operation and Management.

2.15. The Solution should have the capability to export results, reports, and extracts in all the standard formats like csv, pdf, xls and any other feasible formats.

2.16. Dashboards may be provided through console or any other recognized/ reputed MIS Tool at no extra cost. Some of the reports required as part of MIS are as given below:

(a) User-defined reports should be provided as per requirements.

(b) Report can be generated location wise and any other standard reports as well as customized reports for better MIS and management.

(c) Specific / custom reports will have to be provided within seven days from the time of request raised.

(d) Reports should display no. of provisioned ZTNA licenses, including its utilisation and validity.

(e) User-wise reports shall be generated having licenses utilisation and application access.

2.17. The setup and infrastructure should be designed to achieve and maintain a minimum uptime of 99.98%. This level of availability is essential to ensure continuous operation and minimize disruptions, thereby supporting the overall reliability and performance of the system.

2.18. Solution should be able to capture and display all system, user and Audit logs (either in sequence or by event type) in a simple, intuitive interface to understand the Audit trail.

2.19. Bidder shall ensure that data protection measures are in place, including encryption of sensitive data both at rest and in transit.

2.20. The Solution should support scalability to support geographically separated infrastructure to be managed centrally without having to replace software and only via addition of relevant modules.

2.21. The hardware sizing should be done considering the technical specifications mentioned in Section 9 of this bid document. The Bidder shall provide additional hardware and related active and passive components required to meet the requirement at any time during the Contract period at no additional cost to purchaser.

2.22. Bidder shall ensure regular backup of the solution on pre-defined schedule as per the requirement of purchaser.

2.23. The Bidder shall demonstrate the backup and restore testing on-demand.

2.24. The Bidder must Supply, install and implement ZTNA licenses including its maintenance, administration, Operation support, up-gradation, enhancement of Servers (database, backup solution, server etc), in accordance with submitted Bid, including overall infrastructure with no additional cost during the entire Contract period.

2.25. The Bidder shall provide detailed implementation plan, project readiness and design including HLD, LLD for implementing the proposed solution prior to the commencement of each Phase, which should be duly approved and endorsed by the respective OEM for the solution.

2.26. The Bidder shall carry out and submit a comprehensive evaluation report of security of solution after Go-Live. The evaluation report shall articulate all the security concerns related to weaknesses in design, implementation and operation, and how the same are mitigated by applying appropriate countermeasures, as suggested by a Threat Modelling, MITRE CWE, MITRE CAPEC etc.

2.27. The MSP shall provide the 24x7x365 support for Implementation, Integration, and Operation for supplied solution during the Contract period.

2.28. Software, hardware, licenses, AMC, management, maintenance, development, warranty, patching will be responsibility of the bidder during the Contract period and any extension thereof.

2.29. The solution must include a Disaster Recovery site located within the Purchaser's Data Centre for the on-premises solution and must adhere to audit compliance mentioned under 4.7 Audit

2.30. Any additional hardware, system software like enterprise operating system, database, automation etc. required to run the solution shall be factored by the Bidder with 24X7 support, back lined with respective OEMs at no additional cost to the Purchaser. This is applicable to both Primary and DR sites.

2.31. Ensure baseline security hardening of MSP supplied and deployed ZTNA solution as per Centre of Internet Security (CIS) benchmarking before Go-Live.

2.32. The solution required for protecting/securing the bidder supplied and deployed endpoint security solution, shall be provisioned by bidder at its own cost.

2.33. Responsibility of removal of the existing agents from the endpoints before deployment/provisioning of new solution lies with the bidder.

2.34. The MSP shall ensure, no telemetry data leave from the Purchaser's data centre (DC, DR).

2.35. The MSP shall not use the data/telemetry/metadata collected from the ZTNA instance of Purchaser for any purpose other than providing the services under the scope of this Bid.

2.36. The solution shall provide real time streaming of logs to Purchaser logging platform without any pre-processing or filtering at source. The raw logs shall include such as User Authentication, Transaction, Application, Audit Logs, any changes in configuration/updation etc.

2.37. Solution log data must be stored in a compressed and encrypted form and shall support storage of logs for rolling period of 180 days within the supplied solution.

2.38. The proposed ZTNA solution must support banner customization, allowing Purchaser to adapt the banner to align with their unique branding, security policies.

2.39. The proposed ZTNA solution should send posture failure notifications when a device's security posture fails to meet the criteria for resource access.

2.40. Operational support (viz. regular job execution and monitoring, server Backup/ restoration, technical housekeeping, disk space, training) before and after production deployment Installation.

2.41. The ZTNA agent should support various OS i.e., windows, Linux (such as Fedora, Ubuntu etc), MAC, iOS, Android at the time of the bid submission. Solution should support all the new OS, Updates/Versions within 90 days of release without any additional cost to the Purchaser.

3. Project Timelines

Project Timelines to be adhered by the selected Bidder is defined as below:

TABLE 4: PROJECT TIMELINES

S. No.	Product / Service Delivery	Timeline
1	Issuance of Contract	T
2	Delivery of Hardware & Software for hosting ZTNA Solution as per BoM.	T+8 weeks
3	Commissioning of Hardware & Software for hosting ZTNA Solution.	T+10 weeks
4	Provisioning of ZTNA licenses on Bidder’s supplied hardware in Purchaser’s data centre, as per Contract Note: - 1) All components of ZTNA shall be deployed in Purchaser’s designated Data Centre (DC and DR). 2) Inter-rack communication, rack to switch communication and other aspects related to setup shall be taken care by Bidder.	T + 14 weeks
5	Deployment of all Operational Manpower (Refer Section 11)	T+14 weeks
6	Documentation as per paragraph 4.2	T+14 weeks or earlier
7	1) Security hardening of MSP supplied and deployed solution as per Centre of Internet Security (CIS) benchmarking. 2) Comprehensive Security Audit of the items mentioned in S. No. 4 and fixing of vulnerabilities/ security issues found during the Audit through a CERT-In empanelled Auditor based on the scope of work as approved by the Purchaser,	T+16 weeks

	refer Annex 5 for indicative scope of work.	
8	Successful completion of UAT/Sign Off	T+17 weeks
9	Go-Live	T+17 weeks
10	Complete Migration of— (i) any existing ZTNA licenses of the Purchaser to MSP's supplied hardware in Purchaser's Data Centre if required.	As per the Purchaser requirement.

Note:

a) The key responsibilities of the Purchaser shall include providing the necessary data centre hosting space for racks, along with air conditioning, power supply, and internet connectivity, solely required for the on-premises deployment of ZTNA solution.

b) The Purchaser shall provide the necessary seating space for the personnel assigned to this project.

4. Roles and Responsibility of MSP

4.1 The key responsibilities of the MSP shall include, but not be limited to, the following:

4.1.1 The MSP shall be coordinating with OEMs of all supplied components and integration thereof and continued support during the period of contract.

4.1.2 The MSP is required to share all internal review documents and reports used to monitor and execute the project with the Purchaser upon request and as deemed necessary.

4.1.3 The MSP is responsible for providing all necessary logistical support for the resources deployed at the locations of the Purchaser throughout the period of the contract.

4.1.4 MSP shall position a dedicated technical team (During implementation and UAT) and align OEMs support team to commission and manage the solution provided under this bid document.

4.1.5 For all type of technical support services/premium support & SLA where involvement of OEM is required, there should be a back-to-back Agreement between successful Bidder/MSP & OEM, if OEM itself is not the Bidder. MSP will be the single point of contact and will also provide escalation matrix for OEM of the proposed solution.

4.1.6 The MSP shall provide dedicated Desktop/Laptop for deployed manpower with latest configuration each for Windows, Linux, MAC for troubleshooting OS compatibility issues along with solution.

4.1.7 After commissioning the solution if investigation goes under forensic analysis w.r.t operating systems, servers, computers, laptops, hard drives, mobile phones and other digital devices, digital evidence preservation, recovery, analysis, electronic mail extraction, database etc. then in this case MSP will do the forensic analysis and provide the tools required for forensics analysis of affected devices.

4.1.8 MSP shall ensure to arrange requisites licenses/tools for security of deployed ZTNA solution, at no cost to the purchaser.

4.1.9 MSP shall ensure end to end OEM technical support round the clock for addressing operational challenges, based on the requirement.

4.1.10 The MSP shall provide round the clock support for operations, implementation, integration and maintenance/trouble shooting of the deployed ZTNA solution during the contract period.

4.1.11 The MSP shall perform the DR Drills once every Quarter, periodic backup, load testing and backup restoration activities of the Solution and ensure that the immediate restorable version of the Solution are available for maintaining the data integrity.

4.1.12 It is the responsibility of the MSP to share each, and every requirement mentioned in bid with the OEM. It is the responsibility of the MSP to sign SLA with OEM.

4.1.13 Purchaser will not be responsible for any dispute related to IPR; the entire onus for resolution will lie with the respective MSP/OEM. The Intellectual Proprietary Rights (IPR) of any customizations done for the Purchaser remains with Purchaser.

4.2 <u>Manual and Documentations for MSP</u>:

4.2.1 The MSP shall be responsible for the creation and maintenance of all documentation.

4.2.2 The documentation shall be consistently updated throughout the Contract period, adhering to appropriate change management procedures and version control. It is advisable to follow standards and best practices, when creating the documentation. The documentation shall include, but not be limited to, the following:

(i) Solution architecture.
(ii) Project plan with milestones, resourcing, and deliverables.
(iii) Architecture & design (HLD, LLD) Document including network architecture, Traffic and packet flow document between the devices.
(iv) SOP documents.
(v) Product literature, Operating manuals
(vi) Documentation on troubleshooting.
(vii) Application upgrade and patch management document.
(viii) Testing cases and test results documented before and after implementation.
(ix) Industry best practices, use cases and customization.
(x) Vendor support details and escalation matrix.
(xi) OEM support details and escalation matrix.
(xii) Inventory list consisting of hostnames, make, model, serial number.
(xiii) BCP plan and documentation.
(xiv) Backup Plan and documentation

Note: The above list is indicative, and the MSP must provide customized reports and documents as and when required.

4.3 <u>Training & Support</u>

As a part of deliverables, the MSP shall provide the following trainings:

4.3.1 Two days Operational training on the solution offered:

(i) The MSP shall impart Operational and Maintenance training to at least 100 designated officials of the Purchaser bi-annually first year and subsequently once in year at Purchaser’s location.
(ii) The contents of such training shall be documented and made available to all the Users electronically.

4.3.2 Two days technical training on Design and Architecture of the solution offered:

(i) The MSP to provide comprehensive training annually to the team of at least 10 officials as designated by the Purchaser on supplied solution at Purchaser's location.

(ii) The contents of such training would need to be documented and made available to all the Purchaser for training other officers of Purchaser.

The schedule and content of trainings shall be discussed with the Purchaser at the time of contract.

4.4 Terms and Conditions for Proposed solution

4.4.1 MSP shall ensure that the management and operations of the deployed infrastructure is done through laptops/ desktops approved by the Purchaser for that purpose and not through any other private or public device.

4.4.2 MSP shall ensure that all the software and hardware components which will be used for ZTNA deployment shall be hardened as per standard best practices such as CIS.

4.4.3 MSP shall ensure that only approved manpower has access for ZTNA deployment.

4.4.4 MSP and/or its employees/ representative shall be required to furnish necessary undertaking, NDA before such access is provided.

4.4.5 MSP shall ensure that the entire solution ecosystem is secure and is configured to prevent unauthorised access, in the course of setting up, maintenance and operation of ZTNA solution and shall ensure that services are performed in a protected and secure environment which ensures confidentiality and integrity of the data and artifacts.

4.4.6 Purchaser reserves the right to get the devices used by MSP audited through an agency selected by Purchaser/User Organisations.

4.4.7 The MSP shall ensure services from the OEM to be available 24x7x365 if required during the Contract period.

4.4.8 The Solution should have a report scheduler to auto generate and distribute relevant periodic pre-defined reports to SPOC.

4.5 Manpower Support for 24x7x365 Operations provided by Bidder/MSP

4.5.1 The MSP shall ensure that the deployed solution is supported 24x7x365.

4.5.2 The Bidder is required to submit a resource deployment plan as part of the technical Bid submission, outlining how technically qualified staff shall be allocated to execute the project. Manpower SLA shall be applicable as per the deployment plan submitted the bidder.

4.5.3 The MSP shall be responsible for the monitoring and management of the resources/manpower throughout the project. The plan should include the deployment of manpower on-premises of Purchaser's data centre on permanent basis, and the deputation manpower to visit the on-premises setup for fixing issues. The MSP shall provide daily, weekly and periodic reports, both technical and managerial, to designated persons of Purchaser.

4.5.4 The specific manpower requirements are outlined in (Section 11), which provide only an indication of the minimum number of resources needed to undertake the activities as given in the scope of work. The MSP bears the responsibility of allocating and supplying adequate number of resources/manpower to fulfil the scope of work and ensure compliance to SLA.

4.5.5 Terms and Conditions for Resources/Manpower-

(a) The proposed resources/manpower shall be on the payroll of the bidder/MSP (based on the requirements outlined in section 11) and during their deployment.

(b) The personnel deployed by the MSP under this Contract/Agreement, under no circumstances, be considered employees of the Purchaser. The MSP shall have the sole responsibility for the supervision and control of the personnel deployed in the Project and for payment of such personnel's compensation, including salary, provident fund, withholding of income tax and other taxes, worker's compensation, employee and disability benefits and the like, and shall be responsible for all obligations of an employer, subject to Applicable Law.

(c) The MSP shall designate an experienced and qualified Project Manager as per (Section 11) as a SPOC for the Purchaser.

(d) During the implementation phase, the MSP shall establish a project governance team which shall include the Manpower proposed as part of Technical Bid including Project Manager along with required number of personnel within MSP's hierarchy in order to support the escalation matrix. The project Governance team shall continue to function for entire Contract period. The project governance team shall be responsible for ensuring compliance, conducting reviews, overseeing the project, and providing status reports as defined in the operations manual or any status report as and when desired by the purchaser.

(e) The MSP shall, to the best of its efforts, avoid any change in the team proposed for execution of this Contract or replacement of any resource/Manpower appointed. The MSP shall promptly inform the Purchaser in writing if any such change is necessary. In case of replacement of any resource, the MSP shall ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate handholding period and training for the incoming resource.

(f) If the deployed resources don't possess the required skill set or if the resources are not able to deliver on the assigned tasks, the resources shall be replaced (with similar or higher skill set and experience as specified in the bid document) within 30 days of receiving such intimation from the Purchaser. The Resources are expected to work in a 24x7 security operations environment at the Purchaser location.

(g) Penalties will be applicable as per SLAs (refer table 11) under following conditions.

   i. Absence of an onsite deployed resource
   ii. Resignation/ Replacement of Resource based on confirmation of the Purchaser.
   iii. Use of any other email id/other unauthorised mode of communication is strictly prohibited.
   iv. The resources deployed under this contract shall work for the Purchaser only and shall not be used by the MSP for any other project.
   v. Manpower deployment as per defined timelines (refer Table 4)

(h) The MSP shall provide professional grade laptops with at least 8 Core latest gen 2.4 GHz CPU, 16 GB RAM and 1TB SSD, standalone MS Office professional (latest version) with perpetual license to the deployed resources. The laptops shall not have any DLP, Endpoint security or other any other third-party software. Resource shall not connect these dedicated laptops anywhere outside the Purchaser's network, without the explicit written permission of the Purchaser. This laptop shall be used for the official purposes only. The ownership of the data residing in such laptops shall lie with the Purchaser/Organisation.

(i) In case a Resource of the MSP is no longer associated with this project; the laptop shall be surrendered with the Purchaser for sanitization prior to its assignment to a new Manpower.

(j) The bidder shall be required to provide the documentary proof of the qualifications and experience of the manpower being provided by it during the selection process by the Purchaser.

(k) All manpower shall report to the designated nodal officer(s) assigned by the Purchaser. The MSP must ensure proper planning for backup manpower to comply with the SLAs. This backup manpower must possess equivalent qualifications and experience as the person(s) they shall replace.

(l) MSP shall furnish the proof of employment of the manpower on the payroll of the MSP as and when requested by the Purchaser.

(m) The MSP shall carry out background checks of the resources identified to work on this project and submit the background check reports, along with copies of any of the officially valid documents in respect of each such resource. The Purchaser shall also extend necessary cooperation, which may extend to disclosure of income-tax Permanent Account Number and other identification details, professional history including directorships, disclosure regarding criminal prosecution if any and organisational affiliations, and shall require any resources as aforesaid to so cooperate, for such person to undergo security vetting by such government-designated agency as the Purchaser may communicate in writing. If the Purchaser communicates in writing the fact of a resource having been identified as unsuitable by such agency as aforesaid, at any point of time, the MSP shall take action to promptly revoke all the access related to project on immediate basis and remove such resource from the project immediately in any case not later than 24 hours from the receipt of such communication.

The Purchaser shall have the authority to remove any person employed at the Project site who carries out duties incompetently or negligently.

4.6 Product Support (Components and Software)

4.6.1 The MSP must ensure the product(s) supplied as part of the Contract are supported from the respective OEMs for the period of the contract, MSP shall ensure to arrange requisites licenses/tools for security of deployed ZTNA solution, at no cost to the purchaser and any extensions thereof, as provided for in the contract, starting from the date of completion of installation and commissioning of the product(s) delivered.

4.6.2 The licenses supplied as part of the solution deployed, shall also include timely supply and deployment of all their upgrades & updates for the entire Contract Period, and any extension thereof. The MSP should also ensure that the latest versions recommended by OEM in the Solution are configured in the production at any point of time during the Contract period.

4.6.3 The MSP must ensure that product(s) supplied as a part of the solution is/are always of the latest version and any replacement/upgrade of the product that shall ensure better delivery of Service to the Purchaser shall be made available to the Purchaser at no additional cost.

4.6.4 During the Contract Period, if the component/subcomponent goes end of life during the validity of contract, then the MSP shall upgrade the component/ sub-component with an alternative that is acceptable to the Purchaser at no additional cost to the Purchaser and without causing any performance degradation.

4.6.5 Any additional hardware or software required to run the solution as per the contract issued shall be factored by the Bidder with 24X7 support, back lined with respective OEMs at no additional cost to the Purchaser. This is applicable to both Primary and DR sites.

4.6.6 The Purchaser shall not bear any responsibility for disputes related to Intellectual Property Rights involved in supply/use of the product(s) supplied, and which is not owned by the Purchaser. The Purchaser is not responsible for resolution of such disputes.

4.7 Audit

4.7.1 The MSP shall ensure the following audits and assessments**:**

(a) Security Assessment: The MSP shall get the comprehensive security audit of entire solution (including all MSP supplied and deployed components) done annually as per scope of work (Refer Annex 5 for guidelines for Cybersecurity audit) through a CERT-In empanelled third-party auditor and submit the compliance to the Purchaser within two weeks of submission of the audit report by the Auditor. The cost for the same shall be borne by the MSP. MSP shall also get the re-verification audit by CERT-In empanelled auditor for verification of patching of vulnerability / closure of gaps and submit report within one month from the date of submission of the comprehensive security audit report by the Auditor.

(b) Forensic Investigation: Purchaser reserves the right to initiate a forensics investigation of the ecosystem deployed by the MSP through a 3rd party auditor, annually and in case of specific inputs received from investigating agencies with the required evidence. The cost for such audit shall be borne by the MSP. If the forensic investigation report identifies issues due to lapses in implementation and compliance by the MSP and there are two such events wherein a lapse is found, the Purchaser reserves the right to invoke the Termination, forfeit the PBG.

4.7.2 **Limited Audit** - The MSP must conduct a half yearly internal limited audit at its own cost and submit the compliance to the Purchaser within two weeks of submission of the audit report by the Auditor. Refer Annex 5 for guidelines for Cybersecurity audit.

4.7.3 The MSP shall comply with the directions of the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC) regarding reporting of incidents to them, through the Purchaser, within six hours of such incidents coming to or being brought to its notice. The MSP shall highlight any relevant logs to the Purchaser in case of any security issues as soon as the MSP becomes aware of the same.

4.7.4 All types of data created during the performance of this bid document shall be owned by the Purchaser. The MSP shall take the utmost care in maintaining security, privacy, data sovereignty, confidentiality and back-up of such data. Access to the data or systems shall be given by the MSP only to their authorised representative(s) and their names and contact details shall be shared with the Purchaser in advance. Purchaser's authorised representative(s) may conduct periodic or surprise security reviews and audits, with a view to ensure compliance with the provisions of this Agreement by the MSP for data and system security and the MSP shall facilitate extraction of all types of logs as and when required by the Purchaser.

4.7.5 In case an RCA carried out by the Purchaser or surprise security reviews and audits conducted by the Purchaser's authorised representative(s) reveal non-adherence to minimum Service Levels as attributable to any act or thing required to be done or omitted to be done by the Bidder, the corresponding SLA parameter shall be reckoned on the basis of such finding of non-adherence, irrespective of any measurement done, report given or RCA carried out by the Service Provider. Further, in case such finding is at variance with the measurement done, report given or RCA carried out by the Bidder

(a) such non-adherence shall be remediated by the MSP within 48 hours, and the corresponding reports shall be rectified by the MSP and submitted to the Purchaser; and

(b) if the Impact Level of any SLA reckoned on the basis of that finding is higher than that reckoned on the basis of the measurement done, report given or RCA carried out by the MSP on more than two occasions, the MSP shall bear the cost of the RCA carried out or the surprise security review or Audit conducted by the Purchaser, as the case may be, for every such occasion beyond the second such occasion.

4.8 User Acceptance Testing

4.8.1 The MSP shall prepare UAT Document comprising of test cases for functional and performance testing and submit the same for validation and sign off by the Purchaser. The MSP shall ensure that all the test scenarios are identified and provide comprehensive coverage of all aspects. If any additional test cases are required by the Purchaser, the same shall be included by the MSP and the revised UAT Document shall be resubmitted for validation and sign off by the Purchaser. The signed off UAT Document shall be used for the tests and the results shall be provided to the Purchaser for acceptance.

4.8.2The UAT process shall incorporate the below indicative list of stages given below:

(a) Submission of documentations including design, architecture, configuration, troubleshooting, Standard Operating Procedure, etc.
(b) Test Planning and preparation of test scenarios and test cases
(c) Testing
(d) Reporting
(e) Reviewing
(f) Sign-off

4.8.3 The User Acceptance Testing (UAT) shall be conducted by the bidder, after the installation, commissioning and integration has been completed in accordance with the requirements specified in the bid document, in the presence of the Purchaser. The MSP shall take remedial action to rectify any deficiencies/ shortcomings observed during UAT or as indicated by Purchaser. MSP shall submit a duly signed UAT report for validation and sign off by the Purchaser.

4.8.4 Any tools used during UAT; configuration of such tools shall be certified by respective OEM.

4.9 Price Stability

4.9.1 The prices quoted by the Bidder shall remain firm and fixed, without any escalation or revision for whatsoever reasons, till the completion of contract period including the extension period (if any).

4.10 Earnest Money Deposit by Bidder

4.10.1 EMD shall be as per GeM Terms & Conditions.

5. Bid Submission

5.1 Bid shall be submitted as per the GeM Terms & Conditions.

5.2 Bidders are advised to study the bid carefully. Submission of Bid shall be deemed to have been done after careful study and examination of the bid Document with full understanding of its implications.

5.3 Conditional Bids shall not be accepted on any ground and shall be rejected straightway. (A Bid is conditional when Bidder submits its Bid with his own conditions & stipulations extraneous to the terms and conditions specified in this bid).

6. Evaluation of Bid

6.1 Pre-qualification Criteria

6.1.1 The Bidder and OEM must possess the requisite experience, strength, and capabilities in providing the products and services necessary to meet the requirements as described in the bid document. The Criteria are as below:

(a) The Bidder must meet the qualification criteria defined in Table 5 (Bidder Pre-Qualification Criteria) of this bid document.

(b) The OEM of the respective Solution Provider must meet the qualification criteria defined in Table 6 (ZTNA OEM Pre-Qualification Criteria) of this bid document.

(c) If any OEM bids as Bidder, it will also have to qualify the qualification criteria defined in Table 5 (Bidder Pre-Qualification Criteria) of this bid document.

(d) All documents provided by the Bidder shall be signed by Authorised Signatory of the bidder and all documents provided by OEM should be counter signed by Authorised Signatory of the bidder.

Note:

(a) Any Bid failing to meet any of the required above qualification criteria shall be disqualified.

(b) Consortium and Sub-contracting are not allowed in this bid.

(c) In case parent entity/group company experience by the bidder, proof of relationship between Bidder and parent entity needs to be submitted duly signed by Authorised Signatory of the Bidder.

TABLE 5: Bidder Pre-Qualification Criteria

S. No.	Category	Criteria	Documents Required	Yes/No (Page no. in technical bid)
1.	Legal Entity	The Bidder must be incorporated and registered in India under the Indian Companies Act 1956/2013 LLP Act 2008 / Partnership Act 1932 & subsequent amendments thereto and shall have been operating for the last three years as on 31st March 2025 (including name change/ impact of mergers or acquisitions).	Valid documentary proof of: i. Certificate of incorporation / Certificate of Commencement ii. Certificate consequent to change of name if applicable. iii. Copy of Memorandum of Association (if applicable) (In addition, the Bidder shall also submit last 3 Audited balance sheets.)	

S. No.	Category	Criteria	Documents Required	Yes/No (Page no. in technical bid)
2.	Identity Proof	The Bidder must have a registered number of: - GST Registration. - Income Tax number / PAN / TAN.	i. Certificate of GST registration. ii. Copy of PAN / TAN / Income tax number.	
3.	Financial: Turnover	The Bidder must have an Average Annual Turnover of not less than INR 300 crore (Three Hundred Crores) in any three consecutive financial years from FY 2021-22, 2022-23 ,2023-24 and 2024-25 from ICT/Cloud services/Cyber Security services. Note - This must be the individual company turnover and not of any group of companies.	Copy of audited profit and loss account and balance sheet of the three Financial Years and Certificate from statutory auditor/CA quantifying `the average Annual revenue from the ICT/Cloud services/Cyber security related services.	
4.	Financial: Net Worth	The Net worth of the Bidder in any three consecutive financial years from FY 2021-22, 2022-23 ,2023-24 and 2024-25 must be positive. The net worth of the bidder should not have been eroded by more than 30% (thirty percent) in the last three financial years.	Audited Balance Sheets for the three consecutive financial years out of the following: (a) 2021-22 (b) 2022-23 (c) 2023-24 (d) 2024-25 where financial turnover is segregated. Every sheet shall be duly certified by a chartered accountant or accounting firm stating Net Worth, Turnover and Profit/Loss for the three financial years.	
5.	Authorisation	Authorization of signatory for the purpose of this bid	Letter of Authorization/Power of Attorney/Board Resolution	
6.	Non-Blacklisting Undertaking	The Bidder must not have been blacklisted by Government of India or by the Department of	Self-certification by the Bidder duly signed by the Authorised Signatory of	

S. No.	Category	Criteria	Documents Required	Yes/No (Page no. in technical bid)
		Expenditure or by Ministry of Electronics & IT or by NIC on the date of submission of the bid. Bidder also must not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry / Department/ PSU/ Government Company.	the Bidder on Bidder's firm letter head.	
7.	Presence in India	The Bidder should have a permanent office in India as on bid publishing date.	Self-Declaration from the Authorised Signatory	
8.	Land Border Sharing	Any Bidder from a country which shares a land border with India will be eligible to bid in this bid only if the Bidder is registered with the Competent Authority (i.e., Registration Committee constituted by Department for Promotion of Industry and Internal Trade (DPIIT)).	Declaration by the Bidder on their letter head that the Bidder has proposed no such Solution in response to the bid.	
9.	OEM Authorization Certificate	Bidder should provide valid OEM Authorization Certificates for all the proposed solution as well as certify that the proposed product is not declared end of sale.	The bidder shall submit the MAF certificate in reference to this bid document, duly signed by the authorised signatory of the OEM.	
10.	OEM Support	Bidder should provide back-to-back premium support from OEM for entire contract period from the date of Go-Live via IVRS, email, web site.	Undertaking from Bidder by the Authorised Signatory.	
11.	Resources deployed	The resources deployed shall not be used by the Bidder for any other project.	Undertaking from Bidder by the Authorised Signatory.	

S. No.	Category	Criteria	Documents Required	Yes/No (Page no. in technical bid)
12.	Make in India (MII) Purchase Preference	MII Purchase Preference	Undertaking from Bidder on compliance of MII order 2017 and its latest amendments issued by DPIIT duly signed by the Authorised Signatory.	

TABLE 6: ZTNA OEM Pre-Qualification Criteria

S. No.	Category	Criteria	Documents Required	Yes/No (Page no. in technical bid)
1.	OEM Presence	OEM should be operating in India for at least three years as on Bid submission date.	OEM Self-Declaration from the Authorised Signatory.	
2.	Experience	(i) OEMs for the respective ZTNA Solution must have supplied and successfully deployed and maintained at-least 80,000 licenses during the last three financial years for any Central / State Govt Organization / PSU / Public Listed Company /Banks in India. (Global experience will be considered/evaluated only if relevant, verifiable references are submitted along with the bid. (ii) OEM for the respective ZTNA Solution must have supplied and successfully deployed and maintained 20,000 licenses in India to any Central / State Govt Organization / PSU / Public Listed Company/Bank in last three financial years. Copies of relevant contracts to be submitted along with bid in support	Copy of purchase order/Contract and Certificate of completion of the work from clients to be submitted. The documents should clearly establish the required period of experience. All the provided references shall be verifiable. Following details must be provided for references— (i) Name of Client/organisation (ii) Name of contact person (iii) Designation in organisation (iv) Email id	

S. No.	Category	Criteria	Documents Required	Yes/No (Page no. in technical bid)
		of having supplied some quantity during each of the financial year.		
3.	Compliance to Features	All the features listed in the Section 9 of this bid should be ready on the date of submission of the bid.	(i) OEM Self-Declaration, from the Authorised Signatory for compliance with all the points mentioned in the Section 9. (ii) Undertaking as per Annex 4.	
4.	Non-Blacklisting	The OEM must not have been blacklisted by Government of India or by the Department of Expenditure or by Ministry of Electronics & IT or by NIC on the date of submission of the bid. OEM also must not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry / Department/ PSU/ Government Company.	Self-certification by the OEM duly signed by the Authorised Signatory of the OEM on OEM's firm letter head	
5.	Malicious Code Certificate	The OEM shall certify that the Hardware and the Software being offered, as part of the Contract against referred bid, does not contain embedded malicious code.	Certificate to be submitted using Annex-6	

Note:

(a) The bidder shall submit the above-mentioned OEM specific documents duly signed by the authorised signatory of the OEM as part of the Bid.

(b) Any Bid failing to meet any of the required above qualification criteria shall be disqualified.

(c) Any single company participating as both Bidder & OEM will have to independently fulfil all the prequalification criteria as mentioned in the bid document.
(d) All certificates requested in the bid should be valid as on date of bidding.
(e) If OEM is participating as a bidder, the OEM will have to submit all the required documents as mentioned in the bid document.

6.2 Technical Evaluation Criteria

6.2.1 Purchaser will review the technical bids of the participating bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at Purchaser discretion.

6.2.2 The decision of the Technical Evaluation Committee in the evaluation of Bids shall be final. No correspondence will be entertained outside the process of evaluation with the Committee.

6.2.3 Only those bidders who qualify both the Pre-Qualification Criteria and the OEM's Pre-Qualification Criteria will be called for the technical presentation and demonstration.

TABLE 7: Technical Evaluation Criteria

Sr. No.	Technical Evaluation Parameters	Evaluation Criteria	Required Documents / Basis of Evaluation	Yes/No (Page no. in technical bid)
1	The Bidder must have experience of successfully completing/ ongoing project for implementation of ZTNA technology /Cyber Security services in the last three Financial Year (2022-23, 2023-24,2024-25) and up to date of Bid submission.	Contract value for providing ZTNA technology /Cyber Security services: The cumulative contract values of last three financial years shall be more than INR 100 Crores, including 1 contract of at least 10 crores.	Copies of relevant Contracts or Client Certificate/ Agreement/ Contract documentation depicting the said experience credentials must be submitted. In case of NDA, A masked Contract/contract/Agreement /CA certificate with relevant details to be provided. Note: Value of Contract will be considered as inclusive of all taxes. **Note:** Work Completion certificate is mandatory. For Ongoing project: Certificate to the effect shall have to be provided from the Client clearly defining the name, address, contact person, and contact number, email address and scope of work	

2	Bidder experience in offering Managed Services of end point (desktop/laptops) services, in the last three Financial Year (2022-23, 2023-24,2024-25) and up to date of Bid submission.	Experience of running Managed Service for — More than 20000 end points	Copies of relevant Contracts or Client Certificate/ Agreement/ Contract documentation depicting the said experience credentials must be submitted. In case of NDA, A masked Contract/contract/Agreement /CA certificate with relevant details to be provided.	
3	The Bidder should have technically skilled employees based in India on own pay roll of the company at the time of Bid submission.	Minimum 100 Technical resources	Certificate from the statutory auditor/a practicing Chartered Accountant/Company Secretary/ authorised signatory of bidder.	
4	The Bidder must have OEM Certified technical support professional on its permanent roll in India, of proposed ZTNA solution, at the time of Bid submission	Minimum 20 OEM Certified resources	Certificate from the statutory auditor/a practicing Chartered Accountant/Company Secretary/HR regarding such EPF-enrolled employees, along with a list of such employees signed and stamped by authorised signatory of bidder.	
5	Certifications	The bidder should (Valid) CMMi5 certification ISO 9001: 2015 (or latest) or ISO 27001: 2022 (or latest) certification	Copy of Valid Certificate signed and stamped by Certificate from the statutory auditor/a practicing Chartered Accountant/Company Secretary.	
6	Technical Presentation and demonstration: The Bidder needs to demonstrate the solution as per the technical requirements described in this Bid document.	Understanding of the project scope (i) Design and architecture of the proposed ZTNA solution (ii) Overall security measure for the proposed ZTNA solution and Implementation Plan for Securing the Deployment from security threats	Demonstration/Presentation by the prospective Bidder	

		(iii)Additional features related to solution proposed (iv) Comprehensive approach for the operations and maintenance of the supplied solution. (v) Availability of OEM support infrastructure of the proposed solution shall be availability within India. (vi) Proposed implementation strategy as per quoted number of racks and power. (vii) ZTNA Solution scalability and related architecture to meet Purchaser's requirements.		

Note:

(a) Compliance with all the specifications mentioned above must be supported by relevant and verifiable documents.

(b) All supporting documentation for value added features, specifications and sizing of supporting components and CVs of Proposed Manpower as mentioned in the table above, are to be submitted as part of the Technical Bid.

(c) TEC may ask the bidders, if required, for Proof of Concept (POC) of the Proposed ZTNA solution with a week notice. Integrated POC will be based on the following conditions:

(i) POC will be carried out at Purchaser/Bidder/OEM premises during technical evaluation process.

(ii) Bidder may demonstrate all features a functionality as listed in this bid document.

(iii) Any cost associated with demonstrating Integrated POC will be borne by the bidder.

(iv) TEC reserve its right to extend / shorten the period of POC where needed.

(v) Bidders who have failed in the Integrated POC will automatically stand disqualified technically.

6.3 Final Bid Evaluation (Selection of MSP)

6.3.1 The bidders who will qualify technical evaluation stage will be considered for financial evaluation and the financial bid shall be opened electronically on a specified date and time.

6.3.2 Bid will be processed for Reverse Auction as per the GeM terms and conditions. Subsequently, L1 will be declared post completion of reverse auction process.

6.3.3 Component wise price of detailed financial bid of selected bidder will be calculated on pro-rata basis for finalised L1 price in case of reduction in GTV after completion of the RA process.

NOTE: In case of any mismatch in the GTV quoted in Annex 2 and the Grand Total Value provided by the Bidder on the GeM Portal, the discrepancy between these two values shall be removed as per para 6.3.4.

6.3.4 In the event of any mismatch in the GTV value provided at Annex 2 (Grand Total Value) and GTV of the Annex 3 (Detailed Financial Bid), the following criteria shall be adopted to remove the discrepancy between these two values:

a) When Grand Total Value given in Annex 2 (Grand Total Value) is greater than the Grand Total Value given in Annex 3 (Detailed Financial Bid), the value given in Annex 3 (Detailed Financial Bid) shall be taken as the final quoted value by the Bidder and the same shall be accepted by the bidder, before signing of the contract. In case, the bidder does not accept the revised value, the Purchaser reserves the right to reject the bid and forfeit the EMD.

b) When Grand Total Value given in Annex 2 (Grand Total Value) is less than the Grand Total Value given in Annex 3 (Detailed Financial Bid). The value given in Annex 2 (Grand Total Value) shall be replaced with the value given Annex 3 (Detailed Financial Bid) and the item-wise value for each item in Annex 3 shall be reduced on Pro-Rata basis and consequently unit values shall be worked out.

7. Contract Process

7.1 Contract Process

7.1.1 As per GeM Terms & Conditions.

7.2 Performance Bank Guarantee (PBG)

7.2.1 The MSP is required to ensure submission of PBG equivalent to 5 % (Five Percent) of the Contract within 15 days of issue of contract.

7.2.2 Terms and Conditions of GeM shall be applicable, with respect to PBG.

8. Payment Terms

8.1 Payment Terms

8.1.1 A pre-received bill (Three copies), along with certificate of satisfactory performance from User Organisation/NIC shall be submitted on quarterly basis in the name of “NATIONAL INFORMATICS CENTRE (NIC)” at NIC, New Delhi.

8.1.2 MSP shall commission the complete solution and will prepare the installation report and get it signed by Authorised Representative with date and stamp. For the overall project commissioning, a duly signed Go-Live certificate shall be submitted by MSP after signing of UAT.

8.1.3 If the MSP fails to deliver, install, provision and migrate any security solution as per schedule, penalty as per SLAs section shall be applicable.

8.1.4 All payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the latest Income-Tax Act.

8.1.5 Payment against Contract will be done as per payment schedule mentioned in Section 8.2 and the cost of subscription of license will be initiated in the quarter after duly certified Go-Live date. If the operational phase starts in between the ongoing calendar Quarter, the payment quarter shall start from the next calendar quarter however the residual amount of the previous quarter shall be calculated on pro-rata basis.

8.1.6 For subsequent Contracts if any, placed during the lifecycle of the contract, the payment quarter will start from the next calendar quarter however the residual amount of the previous quarter will be calculated on pro-rata basis and will be incorporated in the payment of the first quarter, starting from the date of provisioning of additional software subscriptions purchased, with the existing setup.

8.1.7 For the purpose of any payment, the quarter will be the same as the calendar quarter; that is Jan – Mar, April – June, July – Sept and Oct – Dec.

8.1.8 For any licenses, payment due date shall be reckoned from the date of activation of the license on the Purchaser's central server.

8.1.9 Payment will be done after deduction of all applicable Penalties, for the defaults like delay in delivery, delay in completing the installation of all the ordered items, not maintaining SLA etc. (as defined in section 10 of the bid).

8.2 Payment Schedule

TABLE 8: PAYMENT SCHEDULE

S. No	Billing Cycle	Payment Milestone
1.	Hardware and Software used for hosting ZTNA Solution (Refer Annex 3, Table - 13)	70% cost of Hardware and Software used for hosting ZTNA Solution at delivery after deducing Penalties, if any as per Section 10.
2.	One-time cost for Installation, commissioning of all Hardware and Software used for hosting ZTNA Solution (Refer Annex 3, Table - 13)	30% cost of Hardware and Software used for hosting ZTNA Solution including one-time cost for Installation, commissioning of Hardware and Software used for hosting ZTNA Solution Post Go-live after deducing Penalties, if any as per Section 10.
3.	Provisioning of ZTNA licenses as per BoM (Refer Annex 3, Table – 13-A)	25% cost of ZTNA licenses post every quarter. (License cost as per BOM for that year of Operational phase/4). Penalties shall be deducted as per Section 10.
4.	Comprehensive Security Audit of entire supplied and deployed components by (Cert-in empanelled) (Refer Annex 3, Table – 13-B)	Cost of Comprehensive Security Audit shall be paid after submission of Audit compliance report and resolution of findings. Penalties shall be deducted as per Section 10.
5.	O&M including Manpower (Refer Annex 3 Table 13-B)	25% cost of O&M including Manpower post every quarter (cost for O&M including Manpower of operational phase/4). Penalties shall be deducted as per Section 10.
6.	Any cost for Miscellaneous Expenses – (Refer Annex 3 Table 13- C)	Cost of Miscellaneous Expenses shall be paid after GO-Live.

8.2.1 Payments shall be made subject to the following—

(a) Adherence to the project delivery timelines as per Table 4.

(b) The MSP shall provide all necessary documentation related to the Services consumed and any other documents as demanded by the Purchaser. Invoice without any of the said documents shall be deemed incomplete and not acceptable.

(c) The Purchaser shall release the payment for Services rendered and accepted, subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the Contract and meet SLA requirements.

(d) For release of payment for Annual license subscription of the supplied ZTNA licenses, the MSP shall share the required documents from the respective OEM indicating that the Annual ZTNA licenses have been renewed.

8.3 Payment against time-barred claims

8.3.1 All claims against the Purchaser shall be time-barred after a period of three years, reckoned from the date on which payment falls due, unless the payment claim has been under correspondence. The Purchaser shall be entitled to reject such claims.

8.3.2 In respect of any claim where the same is raised without furnishing the documents as required under the Contract and the Purchaser, as a result, is not in position to claim input tax credit under the Applicable Law(s) governing taxation, the MSP shall not be entitled to payment of such input tax credit amount as the Purchaser would not be in position to claim.

9. Technical Specifications

TABLE 9: TECHNICAL SPECIFICATIONS

Sr. No.	Minimum Specifications	Compliance (Y/N)	Cross-Reference
1.	The solution should have all its components deployed on premise (DC and DR).		
2.	Solution and its components such as hardware, software and application software etc must be fully compatible over IPv6 and IPv4 network.		
3.	The Solution must provide secure access to private application through software agent.		
4.	The dashboard should display discovered applications, applications bandwidth usage, detail about successful transactions, real-time events log of user, application, and application gateway.		
5.	Access to Private application access must only be allowed after a complete security posture validation of the user and devices. The device posture check must check for Registry Key, Client Certificate, Domain Joined, Process Check, firewall, Encryption, Detect Antivirus along with AV signature update, OS Version before providing access to application.		
6.	The Solution must check CRLs for verifying the revocation status of certificates used for the decryption of inbound and outbound SSL/TLS traffic.		

Sr. No.	Minimum Specifications	Compliance (Y/N)	Cross-Reference
7.	The Solution must support filtering of traffic on all ports and protocols including all TCP and UDP ports and must support blocking communication based on user, IP, port etc.		
8.	NIC DNS shall be used as part of the solution.		
9.	The software agent must be tampering proof, and it should not be possible to remove the agent without a password. Solution must have a capability to allow using One Time Passwords/Global Password for agent uninstallation.		
10.	The Solution should provide predefined reports or custom build reports for applications, threats, traffic summary, network bandwidth consuming applications, Top application usage, user or group in PDF or csv format.		
11.	The Solution should provide protection against advanced threats like cookie stealing, XSS, Cryptographic Failures, SQL Injection, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failure and malicious active content.		
12.	The Solution should provide device fingerprint information which includes User ID, OS Type, Device Model, Device State, Device ID, UDID, Machine hostname, Profile Name, Agent Version and Owner.		
13.	The Solution should be capable of providing smart analytics and Application availability like health check.		
14.	The Solution must provide exclusive insight into all administrator actions, providing a digital trail of who did what and when.		
15.	The Solution should provide user to application segregation and connect Users to a specific app and limit the lateral movement.		
16.	The Solution must support Zero trust access for on-premises and roaming users. The Solution must support separate deployment of the broker/gateway to cater on premise and roaming users without exposing on-premise user broker/proxy to internet.		
17.	The broker or equivalent Solution must be deployed in multiple pairs at each data centre (DC and DR) to maintain resiliency and high availability in case of any failure. The Solution must support automatic switch-over of service from DC to DR in case of service failure at DC site.		
18.	The proposed Solution should allow BYOD and third-party Users to freely use their own devices to seamlessly and securely access internal apps leveraging any web browser, no Client needed.		
19.	The Solution shall provide secure remote access to private applications hosted on-premises or in customer's Public Cloud using leading tunnelling technologies with an application connector/secure gateway deployed in the Data Centre.		

Sr. No.	Minimum Specifications	Compliance (Y/N)	Cross-Reference
20.	The Solution must support Web & client-based application, (SSH, Webmail, Web Portals, etc.). It should support both TCP and UDP protocols on almost all associated ports.		
21.	The solution gateway/connector must darknet all private applications, without exposing them even to internal Users to reduce the attack surface. It should support minimum throughput of 400 mbps per gateway/connector.		
22.	The Solution should allow integration with multiple IDP simultaneously for a flexibility to use different authentication service.		
23.	Solution should support REST API for integration.		
24.	The solution must support user to devices restriction to control the number of devices for single user. Solution must restrict devices for users as per NIC's policy.		
25.	The solution must support forwarding the details of all enrolled device to SIEM or Syslog server automatically in real time.		
26.	The endpoint software agent/solution of the proposed solution must have a built-in capability of debugging and packet capture for efficient troubleshooting and a better user experience. The packet capture capability must be GUI based, and it should be exported in PCAP format.		
27.	The Solution must ensure an inbound connection-free architecture for secure private application access. Application proxies/Connectors must initiate only outbound connections, reducing exposure to external threats and enhancing overall security.		

Note:
(i) A valid cross-reference - brochure, Datasheet or information, published on OEM's website as proof of the specified requirements. In case the same is not published on OEM's website, a declaration on the letterhead of the OEM duly countersigned by the Legal head of the company.

10. Service Level Agreement and Penalties

10.1 Purpose

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the services which shall be provided by the MSP to the Purchaser for the duration of this Contract and any extension thereof, along with targets and relevant penalties. SLA and penalty are defined in following categories:

(a) Product Delivery and installation
(b) Operational support and Service Requests.
(c) System availability
(d) Security
(e) Manpower

The MSP shall comply with these SLAs during the operations of the system for entire Contract period. All SLAs and corresponding SLA reports shall monitor and delivered to the Purchaser and

User Organisations by the bidder. All SLA shall be monitored using SLA monitoring tool to be provided and commissioned by the MSP before Go-Live.

The SLA monitoring tool should be capable of monitoring and reporting SLA of ZTNA services on all parameters including but not limited to the details furnished in this section. The tool shall support API-based integration with the proposed solution and associated systems to ensure seamless, real-time, and automated SLA monitoring. All SLAs shall be applicable from the date of Go-Live.

10.2 Key definitions of Service and security SLA

10.2.1 Incident

An Incident is an event that result in loss of the confidentiality, integrity, or availability of information that Purchaser's IT system processes, stores, or transmits, OR a violation of government security policies/procedures or guidelines and regulations. Some of the common examples of an incident includes but not limited to the following:

(a) Complete or partial failure of an ICT Hardware or Software or Service
(b) Non-Availability of an ICT Hardware or Software or Service
(c) Cyber Security Breach
(d) Data Loss, Data Leak
(e) Security misconfiguration
(f) Negligence/mishandling of ICT infrastructure by the MSP team.
(g) Violation of existing security best practices and SOP defined by the purchaser.
(h) Any type of Sabotage.

10.2.2 Service Request

A Service Request is a request made to MSP to fulfil a requirement for day-to-day operations as per scope specified in this bid document. Some of the examples of a Service Request includes but not limited to the following:

(i) Request to create/delete or modify user account on the ZTNA solution.
(ii) Request to install/delete/modify ZTNA agent on a user endpoint.
(iii) Request to resolve ZTNA agent related issues which are impacting the user.
(iv) Request to upgrade the ZTNA user agents

10.2.3 Availability/ Up Time

Means the time for which the services and facilities are available for day-to-day operations using the implemented services.

a) Availability is defined as: {(Scheduled Operation Time – Service Downtime)/ (Scheduled Operation Time)} * 100%.

Note: - Downtime requests approved by the Purchaser shall not be considered as Service Downtime.

10.3 SLA Instructions and Severity Levels for Incident

10.3.1 SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements. In case the service levels cannot be achieved as per in the timelines based on severity levels defined below, due penalties shall be applied and can result in a breach of Contract which shall forfeit PBG.

10.3.2 Root cause analysis (RCA) shall be prepared for all cases of Severity 1 incidents causing service unavailability or disruption. The MSP must provide the RCA.

10.3.3 For any exceptions or SLA breach beyond the control of the bidder, the MSP may submit the RCA along with a justification, which may be considered by Purchaser.

10.3.4 For certain incidents, RCA may be carried out by Purchaser.

10.3.5 The MSP should ensure that the supplied solution offer necessary APIs for facilitating the integration and data exchange with the MIS solution.

10.3.6 Any security related incidents and service requests shall be categorized as S1, S2, S3 or S4 based on the impact of the issue as given in the Severity Table number 10.

10.3.7 Purchaser reserves the right to assign a severity type to any event (incident/service request)

10.3.8 Addressing the issue of advanced threats and cyberattacks, the supplied components shall be monitored by the MSP round the clock for any potential threats/risk and the same needs to be detected immediately and resolved within the timelines defined as per their priority type.

10.3.9 MSP must submit quarterly SLA Compliance report to Purchaser including all the supporting reports including component health monitoring.

TABLE 10: SEVERITY TABLE FOR SERVICE SLAS

Severity Type	Description	Impact	Target/ Timelines for closure
S1	Major failure of ZTNA Solution provided by the bidder. This includes severe disruptions involving major failure in the overall operation of the system. There are no usable workarounds available to fix the problem. Such failures may include errors such as general protection fault, system hangs, etc. that prevent further, testing cannot proceed until the error is fixed. These also include complete or partial service unavailability, including incorrect behaviour of the system, security incidents resulting in breach of security etc.	Complete unavailability of the solution.	1. Immediate Action for Resolution of the cause with required findings, and recommendations, corrective & preventive measures – within 30 minutes. 2. Submission of RCA – Within 8 hours 3. Detection of Zero-day vulnerabilities and any malware or security incident which goes undetected.
S2	System is not completely down but some of the features or components are down impacting all or critical users. Users face severe restrictions in the system, irrespective of the cause. Workarounds are time-consuming. System behaviour is inconsistent. Further, testing cannot proceed in the relevant areas until the error is fixed or a viable turnaround is demonstrated. These also include severely degraded	Partial availability of the ZTNA solution to all user Organisations	1. Immediate Action for resolution of the cause with required findings, and recommendations, corrective & preventive measures – within 2 hours 2. Submission of RCA– Within 12 hours

Severity Type	Description	Impact	Target/ Timelines for closure
	system performance, repeat calls (same issue reported at least twice) etc.		
S3	System is functional and features are available, but multiple users/ Organisations are facing severe functional restrictions in the system. Moderate restrictions in the system, irrespective of the cause. There are convenient and readily available workarounds. Only a few Users are affected. Minor errors are to be fixed, but solution is running with available workaround.	Impact on the performance of ZTNA solution OR limits the functionality of the user end points.	1. Resolution of the cause with required findings, and recommendations, corrective & preventive measures – within 4 hours 2. Submission of RCA– Within 24 hours
S4	Individual users in one or more Organisations are facing service downtime or unavailability for Service request fulfilments as per the technical requirements specified in the bid document.	There is no major impact on the working of the user Organisations, but individual user endpoints are facing functionality/performance issues. It will also include individual user's queries/suggestions.	1. Resolution of the cause with required findings, and recommendations, corrective & preventive measures – within 6 hours 2. Submission of RCA– Within 48 hours.

10.4 Penalties on SLA

Applicable penalties are defined in table below:

TABLE 11: PENALTIES ON SLAS

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
1.	Availability	Availability of supplied solution (including MSP supplied hardware, software and the solution deployed)	Measures availability of ZTNA service Availability of ZTNA service for at least 99.98% of time measured quarterly for a 24x7x365 time period. **Calculation**:	Minimum 99.98% up time measured on a quarterly basis for ZTNA Services	NIL	Measured on a quarterly basis and considered for 24x7x365 operations. Any downtime taken with the written approval of the Purchaser shall be excluded
				>= 99.96% to <99.98% up Time measured on a quarterly basis for ZTNA Services	1% of the total quarterly payment	

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
			(a) Calculate Downtime percentage for the quarter (b) Availability percentage = {(Scheduled Operation Time – Service Downtime)/ (Scheduled Operation Time)} * 100%. Based on the uptime percentage calculate the penalty	>= 99.94% to <99.96% up time measured on a quarterly basis for ZTNA Services	2% of the total quarterly payment	from the calculation.
				>= 99.92% to <99.94% up time measured on a quarterly basis for ZTNA Services	4% of the total quarterly payment	
				>= 99.90% to <99.92% up time measured on a quarterly basis for ZTNA Services	8% of the total quarterly payment	
				<99.90% up time measured on a quarterly basis for ZTNA Services	10% of the total quarterly payment	
2.	Operations Support	Time to Resolve – Severity 1 (Time taken to resolve the reported problem.)	For Severity 1, 100% of the incidents should be resolved within 30 minutes of problem reporting.	Number of incident(S) up to 2 with more than stipulated response time.	2% of the total quarterly payment	SLA shall be measured quarterly for each incident individually from the time of incident reporting on 24x7x365 operations.
				Number of incident(S) >3 with more than stipulated response time.	4% of the total quarterly payment	
3.		Time to resolve – Severity 2, 3 and 4 (Time taken to resolve the reported problem.)	100% of incidents should be resolved for Severity 2 within 2 hours. Severity 3 within 4 hours. Severity 4 within 6 hours of problem reporting.	Number of incident(S) up to 2 with more than stipulated response time	0.50% of the total quarterly payment	SLA shall be measured quarterly for each incident individually from the time of incident reporting on
				Number of incident(S) 3-6 with more than	0.70% of the total quarterly payment	

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
				stipulated response time		24x7x365 operations.
				Number of incident(S) >6 with more than stipulated response time	1% of the total quarterly payment	
4.		Number of re-opened incidents	For all incidents that are marked as Resolved by the MSP but are re- opened by the client. This is calculated for all incidents reported within the 30 days.	Number Of reopened incidents <=4	0.30% of the total quarterly payment	SLA shall be measured quarterly for each reopened incident individually on 24x7x365 operations.
				Number Of reopened incidents <=8 & >4	0.40% of the total quarterly payment	
				Number Of reopened incidents >8	0.50% of the total quarterly payment	
5.	Manpower	Penalty for unauthorised absence of onsite resources or failure of MSP to provide replacement as required as per the provisions of the bid document.	Absence of an onsite deployed resource	Penalty at the rate of Rs. 30000 per day of absence of Project Manager and Rs. 5000 per day for all other resources shall be levied on the bidder. The penalty shall be deducted from the quarterly payments with the maximum capping of 10%.		Measured from quarterly attendance of the said resource
6.		The deployed manpower resources shall mandatorily use the email id provided by Purchaser for all	Use of any other email id/other unauthorised mode of communication is strictly prohibited	In the instance of any manpower violating this condition, 1. 0.1% of quarterly	0.1% of the total quarterly payment	

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
		official communications related to The Purchaser.		payments shall be levied for each such instance of violation by a manpower, with maximum capping of 10% of quarterly payments.		
7.		Resignation/ Replacement of Resource based on confirmation of The Purchaser.	1) The MSP shall provide in writing at least 30 days prior to the last Working Day of the deployed resource. 2) The resource shall not be relived without proper exit management and written No objection certificate (NoC) from the Purchaser. 3) The MSP shall replace the resource at its own cost and deploy the new resource for Knowledge Transfer (KT) at least 30 days prior to the last Working Day of the outgoing resource.	1. If any resource resigns or shifted out of deployment location in violation of these terms and 1% of quarterly. payment in case of unavailable for performing duty, with maximum capping of 10% of quarterly payments. 2. If the resource is removed without proper No Objection Certificate (NoC), a penalty of	(1) 1% of the total quarterly payment (2) 0.1% of the total quarterly payment (3) 0.01% of the total quarterly payment	Measured from the date of intimation of resource resignation and last Working Day of the resource in the project/engagement

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
				0.1% of quarterly payments shall be applied for each such resource, with maximum capping of 10% of quarterly payments. 3. A penalty of 0.01% of quarterly payments shall be applied per day for the number of days which are less than the required number of 30 days of Knowledge Transfer, with maximum capping of 10% of quarterly payments.		
8.		The resources deployed shall not be used by the MSP for any other project.	The resources deployed through this bid shall work for the Purchaser only and shall not be used by the MSP for any other project.	If any resource is found to be working on any project/activity, which is not assigned by Cyber Security Group of The Purchaser, then	1% of the total quarterly payment for each such instance, with maximum capping of 10% of	

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
				such manpower shall be immediately terminated from the project. A penalty of 1% of quarterly payments shall be levied, for each such instance with maximum capping of 10% of quarterly payments.	quarterly payments.	
9.	Comprehensive Security Audit	Failure to conduct comprehensive security audit annual and half-yearly audits	The MSP shall get the comprehensive security audit of entire solution (including all MSP supplied and deployed components) done annually and Limited audit (Half-yearly) as per scope of work (Refer Annex 5 for guidelines for Cybersecurity audit) through a CERT-In empanelled third-party auditor and submit the compliance to the Purchaser within two weeks of submission of the audit report by the Auditor.	1 % of respective payment per week delay for 1st month, 2nd Month onwards 2% per week	1% of respective payment per week delay for 1st month, 2nd Month onwards 2% per week maximum capping up to 10%.	Penalty shall be calculated based on 1st year audit completed date, if MSP failed to conduct the 2nd year of Security Audit, penalty will be accounted same date in the particular year.
10.		Closure of the Audit findings	Non closure of the Audit findings as per the severity and timeline specified while raising of such	For each week, or part thereof, of delay in the closure of audit findings as specified in	0.5% of the total quarterly payment	Date of acceptance of Audit closer report.

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
			Audit findings, refer 4.7	Section 4.7, a penalty of 0.5% of the total Quarterly payment shall be deducted with a maximum capping of 10% of Quarterly payment.		
11.	Security	Deployment of latest security patches on all supplied hardware and software components.	Within 24 hrs. from the time the patch was made available by OEM unless an extension is given by the Purchaser in writing to the Bidder.	0.5% of quarterly payments for every 12-hour delay for each individual component, with a maximum cap of 10% of total quarterly payment.	0.5% of the total quarterly payment for every 12-hour delay for each individual component	
12.		Deployment of mitigation measures for preventing the exploitation of unpatched vulnerabilities (whose patch is yet to be released by OEM)	Within 72 hrs. from the time the information about the unpatched vulnerability is received from OEM or through any other source	0.25% of quarterly payments for every 24-hour delay for each individual component, with a maximum cap of 10% of total quarterly payment	0.25% of the total quarterly payment for every 24-hour delay for each individual component	
13.		Deployment of software updates (including BIOS, Firmware, OS, etc.) on all supplied components	Within 7 days from the date of update release by OEM	0.25% of quarterly payments for every 72-hour delay for each individual component, with a maximum cap of 10% of total quarterly payment.	0.25% of the total quarterly payment	

Sl. No	SLA Type	SLA Parameter	Definition & Target	Service Level	Penalty	Measurement Mechanism
14.		Security breach related to the deployed ZTNA solution by the bidder Note: It includes any type of security breach in the solution provided or due to the solution provided by the MSP which includes but not limited to all the hardware, software, tools and negligence of the resources deployed by the bidder	No Security Breach is acceptable either due to the provided solution, which is all integrated services, or in the provided solution which is ZTNA platform/solution.	(i) Penalty of 8% of the Quarterly payment shall be levied for each instance of security breach with maximum capping for 10% of quarterly payment. (ii) More than one such breach (iii) More than two such breaches	(i) 8% of the total quarterly payment (ii) 10% of the total quarterly payment (iii) Purchaser reserves the right to terminate the contract	

Note:

(a) SLA penalties during the operations phase (Post Go-Live) shall be calculated on a quarterly basis and will be deducted from the next payment due, quarterly MIS report shall be submitted by MSP covering all the key details and SLA compliance of all the functions.

(b) If the SLA penalties during the operations phase (Post Go-Live) calculations exceed 10% of the quarterly billing for two consecutive quarters then, notwithstanding anything contained herein, the Purchaser may take appropriate action including

i. Invoke Termination of Contract.

ii. Blacklist from participation in future bids of Purchaser; and

iii. Forfeit Performance Bank Guarantee.

(c) Delay for such period as may be caused by any act of the Purchaser or omission of anything required to be done by the Purchaser shall not be considered when calculating penalty on SLA.

(d) Each SLA as mentioned above is independent and accordingly the penalties shall be calculated.

(e) For certain incidents, RCA may be carried out by the Purchaser (or a Purchaser appointed agency), at its discretion.

10.5 Penalty – Delivery, Commissioning and Integration

The below table illustrates penalties with respect to Delivery, Commissioning and Integration of the ZTNA solution.

TABLE 12: Penalties - Delivery, Commissioning and Integration

S. No.	Penalty Definition	Violation	Penalty Level in Case of Default
1.	Delay in delivery of Hardware & Software for hosting ZTNA Solution.	Any delay in hardware delivery at Purchaser's data centre with reference to the timelines defined in Table 4.	0.1% of the Contract value, for per day of delay, with a maximum capping of 10% of the Total Contract Value
2.	Delay in Commissioning of Hardware & Software for hosting ZTNA Solution.	Any delay in hardware commissioning at Purchaser's data centre with reference to the timelines defined in Table 4.	0.1% of the Contract value, for per day of delay, with a maximum capping of 10% of the Total Contract Value
3	Delay in: Provisioning/Deployment of ZTNA licenses on MSP's supplied hardware in Purchaser's data centre, as per contract Note:- All components of ZTNA shall be deployed in Purchaser's designated Data Centre.	Any delay in provisioning/deployment of ZTNA licenses on MSP hardware in Purchaser's Data Centre with reference to the timelines defined in Table 4.	0.2% of the Contract value, for per day of delay, with a maximum capping of 10% of Total Contract Value
4.	Delay in Go-Live	As specified in Table 4	0.2% of the Contract value, for per day of delay, with a maximum capping of 10% of the Total Contract Value.

Note:

(a) Any delays resulting from actions or omissions by the Purchaser that are necessary for the completion of the contract shall not be considered when calculating penalties on SLA.

(b) ZTNA service unavailability for such period as may be caused wholly by any act of the Purchaser or omission of anything required to be done by the Purchaser shall not be taken into account for the purpose of calculating downtime and penalties shall not be applicable.

(c) MSP shall ensure compliance with the uptime and performance requirements of the project as indicated in the above service level tables. Any upgrades or major changes to the setup shall be planned accordingly, and the MSP shall ensure the service level requirements are adhered to.

(d) If the maximum penalty cap (10%) is breached for Delivery, Commissioning and Integration then the Purchaser reserves the right to Invoke Termination of Contract, Blacklist from participation in future bids of Purchaser, Forfeit Performance Bank Guarantee.

(e) If at any time during performance of the Contract/SLA, the MSP encounter conditions impeding timely performance of the above services/SLA, having dependencies of third party (excluding

OEMs of the supplied components) or the Purchaser, the MSP shall notify the Purchaser in writing immediately with the reasons of delay, its likely duration, and its cause(s).

11. Manpower

The MSP is required to deploy skilled manpower, as specified in the Bid, to meet the SLA and Scope of Work, in consultation with the Purchaser. The MSP shall provide qualified personnel during the operation of the solution, including the services of a Project Manager, L3 Engineer, L2 Engineer, and L1 Engineers, with the qualifications and experience as defined below:

Sr. No.	Positions (On-site)	Minimum Qualifications & requirements	Minimum Number of manpower required for Operations
1	Project Manager (SPOC)	(i) Minimum 10 Years of experience in managing the information security of large Organisations/departments. Should have Graduate/master's degree from a recognized university. (ii) Should be PMP certified, also additional security certification like CISSP/CISM/CISA/CEH will be an added advantage. (iii) Hands-on experience of minimum 5 (Five) Years in cybersecurity operations. (iv) Project Management experience with excellent communication skills. The resources will act as a SPOC for Purchaser and MSP and will be responsible for resolving any queries or issues faced by the users.	01
2	L3 - Engineers Technical Manager	(i) Graduate Engineer in Computer Science/ IT/ MCA with minimum 8 years of experience in implementing, managing, and troubleshooting large size Endpoint Protection/ZTNA/ Threat Hunting/ Forensics. (ii) L3 must have complete product knowledge. (iii) Hand-on experience in E-Mail, ZTNA/ Threat Hunting/ Forensics, product function, features pertain to proposed ZTNA Solution and its equivalent security solution. (iv) Certified L3 (Advance) level Specialist with any reputed ZTNA software, Next-Gen antivirus products Organisations Certified certification.	02
3	L2 – Engineers Technical Lead	(i) Graduate Engineer in Computer Science/ IT/ MCA with minimum 5 years of Experience in Support and implementation of Security Products including antivirus	08

Sr. No.	Positions (On-site)	Minimum Qualifications & requirements	Minimum Number of manpower required for Operations
		solution, Endpoint Protection, ZTNA / Threat Hunting. (ii) Hand-on experience in E-Mail, ZTNA/ Threat Hunting, product function, features pertain to proposed ZTNA Solution and its equivalent security solution. (iii) Certification in any of reputed (OEM's) Antivirus Software solution, ZTNA.	
4	L1 – Engineer's Technical Support	(i) Graduate Engineer in Computer Science/ IT/ MCA with minimum 2 year of experience in Antivirus solution, Endpoint Protection, ZTNA solution. (ii) Desirable Certification on Endpoint Protection Platform/ ZTNA solution.	16 resources (24x7)

Note:

(i) The numbers provided are indicative for the minimum requirements. The MSP is free to provide additional manpower as required to support the operations and maintain the SLAs. The manpower is required during the entire Contract period, or any extension thereof prior to Go-Live. The shifts should be overlapping with minimum one hour of handover period between the shift change. The manpower not working 24x7 shall remain available to work anytime and during holidays also as per project requirements.

(ii) All the manpower deployed as part of this project will be operating from Purchaser's specified location.

(iii) The deployed Manpower shall be fully trained on supported Operating Systems (Linux, windows, MAC, IOS and Android).

(iv) The selected MSP shall setup a centralize service desk to record all user's reported incidents/complaints. The Service Desk shall be reachable via Phone, Email and web portal. Support team shall be available 24x7x365 for the ZTNA services during entire contract period.

(v) The selected MSP shall make sure the service desk team can address and resolving the user reported issues in a timely manner to minimize the downtime

(vi) The selected MSP shall provide a clear escalation matrix for the smooth operation and timely resolution of the reported problem as part of the Bid submission.

12. Annexures

Annex 1 – Instructions to fill the Bill of Material

a) Bidder shall provide all prices as per the prescribed format under this Annexure. Bidder shall not leave any field blank. However, quoting of NIL value/no/dash (-) for any item, as listed in the detailed financial Bid shall imply that the Bidder has quoted zero (0) as rate for a specific item. Quoting of Zero (0) as rate for a specific line item will lead to rejection of the bid.

b) All the prices (including taxes) are to be entered in Indian Rupees ONLY (percentage values are not allowed)

c) It is mandatory to provide breakup of all Taxes, Duties and Levies wherever applicable and/or payable.

d) Purchaser reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated.

e) Purchaser shall consider all Taxes, Duties & Levies for the purpose of Evaluation.

f) For evaluation of Financial Bids, the Purchaser shall make appropriate assumptions to arrive at a common Bid price for all the Bidders. This however shall have no co-relation with the Contract Value or actual payment to be made to the Bidder.

Annex 2- Grand Total Value

Abridged Financial Bid

Bidder Name: ....

Abridged Financial Bid for Submission of Grand Total Value

Prices shall be quoted in Indian Rupees (inclusive of all taxes) and indicated both in figures and words. Price in words shall be considered for evaluation, in the event of any mismatch.

Grand Total Value

Grand Total Value (GTV) in figures	
(Rupees__) in words	

Note: The Bidder shall ensure that the Grand Total Value given in Abridged Financial Bid must match the Grand Total Value given in Detailed Financial Bid.

Place:

Date: Authorised Signatory Name:

Annex 3- Detailed Financial Bid

Detailed Financial Bid

Prices in the Financial Bid (Inclusive of all Taxes) shall be quoted in the following format. All prices shall be quoted in Indian Rupees and indicated both in figures and words. Figures in words shall prevail.

The grand total value shall be derived as below:
Grand Total Value (GTV) = shall be the sum total of the following components, inclusive of all taxes:

Grand Total Value for ZTNA

S. No	Component Name	Amount (in INR)
1	Hardware and Software used for hosting ZTNA Solution (Refer Annex 3, Table - 13) - **B1**	
2	Installation, commissioning of all Hardware and Software used for hosting ZTNA Solution (Refer Annex 3, Table - 13) - **B2**	
3	Provisioning of ZTNA licenses as per BoM (Refer Annex 3, Table – 13-A) -**B3**	
4	Comprehensive security Audit by Cert-In empanelled vendor for entire supplied and deployed solution (Refer Annex 3, Table – 13-B) – **B4**	
5	O&M including Manpower (Refer Annex 3, Table – 13-B) – **B5**	
6	Any Miscellaneous Expenses – (Refer Annex 3, Table – 13-C) - **B6**	
	GTV (B1+B2+B3+B4+B5+B6) in figures	
	GTV (B1+B2+B3+B4+B5+B6) in words	

Place:

Date: **Authorised Signatory Name:**

Bidder Name: ....

TABLE 13: Detailed BoM

S. No.	Item	Unit Cost (in INR), exclusive of price for packaging, forwarding, freight, insurance charges, logistics etc. for deployment at DC and DR	Cost (in INR) with 3 years warranty	Taxes (in INR)	Total Cost for Hardware and Software used for hosting ZTNA Solution (in INR)
		B	C	D	E=(B+C+D)
1	Hardware and Software used for hosting ZTNA Solution. (B1)				
	Item	Unit Cost (in INR), exclusive of price for packaging, forwarding, freight, insurance charges, logistics etc. for Installation, Commissioning at DC and DR		Taxes (in INR)	Total Cost for Installation, Commissioning of all Hardware and Software used for hosting ZTNA Solution
	A1	A2		A3	A4=A2+A3
2	Installation, commissioning of all Hardware and Software used for hosting ZTNA Solution (B2)				
Total Value for Hardware and Software used for hosting ZTNA Solution and Installation, commissioning of all Hardware and Software in Words (inclusive of taxes in INR)				B1+B2	
Total Value for Hardware and Software used for hosting ZTNA Solution and Installation, commissioning of all Hardware and Software in Figures (inclusive of taxes in INR)				B1+B2	

TABLE 13-A

S. No.	Item	Unit Cost in 1st Year (i)	Taxes (in INR) (ii)	Total cost of 1st Year	Unit Cost in 2nd Year (iii)	Taxes (in INR) (iv)	Total cost of 2nd Year	Unit Cost in 3rd Year (v)	Taxes (in INR) (vi)	Total cost of 3rd Year	Total Expected Quantity	Total Cost (in INR)
				G (i+ii)			H (iii+iv)			I (v+vi)	J	K =(G+H+I)*J
3	Provisioning of ZTNA licenses (B3)										3,00,000	
	Total Cost for Provisioning of ZTNA licenses in Words											B3
	Total Cost for Provisioning of ZTNA licenses in Figures											B3

TABLE 13-B

S.No	Item	Cost in 1st Year (i)	Taxes (in INR) (ii)	Total cost of 1st Year	Cost in 2nd Year (iii)	Taxes (in INR) (iv)	Total cost of 2nd Year	Cost in 3rd Year (v)	Taxes (in INR) (vi)	Total cost of 3rd Year	Total Cost (in INR)
4				L (i+ii)			M (iii+iv)			N (v+vi)	O= (L+M+N)
	Comprehensive security Audit by Cert-In empanelled auditor for entire										

	supplied and deployed solution (B4)										
S.No	**Item**	**Cost in 1st Year** **(i)**	**Taxes (in INR)** **(ii)**	**Total cost of 1st Year**	**Cost in 2nd Year** **(iii)**	**Taxes (in INR)** **(iv)**	**Total cost of 2nd Year**	**Cost in 3rd Year** **(v)**	**Taxes (in INR)** **(vi)**	**Total cost of 3rd Year**	**Total Cost (in INR)**
				P (i+ii)			**Q (iii+iv)**			**R (v+vi)**	**S= (P+Q+R)**
5	**O&M including Manpower (B5)**										
	Total Cost for Comprehensive security Audit and O&M including Manpower in Words										**B4+B5**
	Total Cost for Comprehensive security Audit and O&M including Manpower in Figures										**B4+B5**

<u>**TABLE 13-C**</u>

S. No.	Item Name	Unit Cost	Taxes (in INR)	Total cost Incl. GST	Qty.	Total Cost (in INR)
6		**T**	**U**	**V=T+U**	**W**	**X=V*W**
6.1	<Item Name>					
6.2	<Item Name>					
	So on…………….					
Total Miscellaneous Expenses in Words						**B6**
Total Miscellaneous Expenses in figures						**B6**
Grand Total Cost for Hardware and Software, Installation, commissioning of all Hardware and Software, Provisioning of ZTNA licenses, Comprehensive security Audit, O&M including Manpower and Any Miscellaneous Expenses, for hosting ZTNA Solution in Words						**B1+B2+B3+B4+B5+B6**
Grand Total Cost for Hardware and Software, Installation, commissioning of all Hardware and Software, Provisioning of ZTNA licenses, Comprehensive security Audit, O&M including Manpower and Any Miscellaneous Expenses, for hosting ZTNA Solution in Figures.						**B1+B2+B3+B4+B5+B6**

Instructions to the Bidder

a) If a Bidder quotes less than the minimum BoQ specified in Table 3, the Bid is liable to be rejected.
b) At the time of initial deployment, the Bidder/MSP shall size the solution (including any hardware, system software like enterprise operating system, hypervisor, database, automation etc. collectively called as infrastructure) with 25% additional capacity of the minimum infrastructure required with 24X7 support. This is applicable to both Primary and DR sites.
c) The cost required for all the licenses for operationalising and for the security of the entire ecosystem of the supplied components shall be borne by the bidder. This is applicable to both Primary and DR sites.

Note:

(a) The MSP shall provide comprehensive technical support services of enterprise class for all the software supplied as above for the entire period of the contract and any extension thereof. The technical support shall include timely upgrades, updates and patches that are released by the respective OEMs during the contract period and any extension thereof.
(b) If the contract is to be extended beyond three years, the Subscription cost of licenses shall be considered based on the third year's cost in 4th and 5th years.
(c) If the contract to be extended beyond three years, the AMC cost for 4th and 5th years shall be calculated at 8% of the unit cost for supplied Hardware and Software for hosting ZTNA Solution.
(d) If the contract to be extended beyond three years, O&M including manpower cost shall be calculated as below.
    (a) 4th year cost = 3rd year cost + Average cost increment of last two years.
    (b) 5th year cost = 4th year cost + Average cost increment of last three years.
    Example for reference is as below:-

1st year cost	**2nd year cost**	**3rd year cost**	**4th year cost**
100	108	118.80	129.50
Increment %	8%	10%	9% (8%+10%)/2)

(e) If the contract is to be extended beyond three years, NIC shall pay the cost of third year's Comprehensive security audit (Cert-In empanelled auditor) for 4th and 5th years.
(f) The unpriced BOM shall not deviate from the one submitted in the financial Bid, or it may lead to rejection of the Bid. Bidder to ensure that unpriced BOM submitted as part of the technical Bid does not include any pricing or financial details.

Annex 4 – Undertaking to be submitted by OEM/Bidder

UNDERTAKING

This is to certify that:

(a) The vulnerability details of the supplied products (product name) shall be shared with the Purchaser prior to public disclosure. The information shall be shared within seven days of such vulnerability details of the supplied products are known to the OEM.

(b) The OEM/BIDDER shall also provide the Purchaser with the necessary information for mitigating any unpatched vulnerabilities identified in their products at no additional cost to the Purchaser.

(c) The OEM/BIDDER shall not use the data/telemetry/metadata collected from the ZTNA instance of NIC for any purpose other than providing the services under the scope of this bid document.

(d) The overall solution architecture (enclosed herewith) including the unpriced bill of materials (enclosed herewith), architecture, sizing, security and deployment of hardware, software, network, security, storage and other relevant components, which are submitted as a part of the technical solution by _M/s.___________________ (Name of Bidder) conforms to the best practices and satisfies all the technical and SLA compliance requirements as per the bid __________________________________ (name of bid for which the solution is being quoted) and international best practices, including the OEM's best practice guidelines. The following solution have been supplied as part of the Bid:

1.___________________

We undertake full responsibility for the solution architecture, design, sizing proposed by the Bidder M.s/________________ in their technical Bid submitted for the bid ____________________________ (Name of the bid document).

We hereby confirm that the solution supplied for which MAF has been submitted as part of this Bid shall not be End of life and End of support and OEM shall provide premium support for period of contract (not exceeding 5 years) from the date of delivery to the Purchaser.

Submitted on behalf OEM Name:

Name of Authorised Signatory:

Designation of Authorised Signatory:

Signature & Seal of the OEM Authorised person:

Place:
Date:

Annex 5 - Guidelines for Cybersecurity audit

1. Comprehensive security 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 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 authorised 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);
(d) penetration testing.
(e) network and device configuration review.
(f) application hosting configuration review.
(g) database security assessment (including whether personal data is being encrypted at rest and in motion, 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 authorised 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,* with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-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 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-empanelled 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.

1.4 Audit shall be based on policy outlined (evidence based) and architecture-based audit.

1.5 Review of previous incident report / audit reports / alerts given by NCIIPC / CERT-In/ other agencies shall be carried out by the Bidder.

2. Limited audit

2.1 Limited Audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is—

(a) modification in application functionality; or

(b) addition/modification of APIs; or

(c) migration to new infrastructure platform or cloud service; or

(d) change in configuration of application hosting, servers, network components and security devices; or

(e) change in access control policy.

2.2 The scope of limited Audit should include, *inter alia,* the following:

(a) *In all cases:* Source code assessment; application security assessment (both Black Box and Grey Box testing) including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis.

(b) *In case limited Audit is after six months of comprehensive audit:* In addition to (a) above, user access controls (including privilege access management) and access reconciliation review; identity and access management controls review.

(c) In case limited Audit is done earlier: In addition to (a) and (b) above, —

(i) For Audit on modification in application functionality, addition/modification of APIs, migration to new infrastructure platform or cloud service or change in configuration of application hosting, servers, network components and security devices: Network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorised 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 tokenised 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 authorised Users and are protected with multi-factor 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-2021-0004]"); security operations and monitoring review (including maintenance of security logs, review of logs, integration with security monitoring solution, correlation and analysis; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law); review of logs, backup and archival data specifically for access to personal data; review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website); and

(ii) *For Audit on change in access control policy:* Review of logs and integration with security monitoring solution.

2.3 Auditor should be a CERT-In-empanelled Auditor who is other than the Auditor who has done the last comprehensive audit. Further, in case the application is hosted on cloud, the Auditor should have capability for carrying out cloud security Audit as per the empanelment details available on CERT-In's website.

2.4 Alternatively, in case there is an information security Audit vertical of the organisation hosting and/or managing the application which—

(a) satisfies the baseline requirements specified for CERT-In empanelment in CERT-In's Guidelines for applying to CERT-In for Empanelment of IT Security Auditing Organisations; and

(b) is independent of the ICT vertical, with the head of such vertical having direct reporting line to the head of the organisation, such information security Audit vertical may perform internal audit.

3. Role of the application owner

3.1 The application owner (Ministry/Department/organisation/agency concerned, as applicable) should—

(a) appoint the Auditor and initiate the Audit process as required.

(b) extend necessary support and access for the audit.

(c) meet the cost of audit; and

(d) ensure requisite follow-up for closure of Audit findings, including in terms of securing requisite approvals and resources and coordinating among the application developer, application manager, hosting service provider, Web Information Manager / Chief Information Officer and CISO.

Annex 6 – Malicious Code Certificate

(To be provided on OEM letter head)

Tender Ref. No.: ________________________________ & Date: ___________

To,
Tender Processing Section
National Informatics Centre
A Block, CGO Complex
Lodhi Road, New Delhi – 110003

(a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code/ malware or trojan that would activate procedures to:
i. Inhibit the desires and designed function of the equipment.
ii. Cause physical damage to the user or equipment during the exploitation.
iii. Tap information resident or transient in the equipment/network.

(b) The firm shall be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.

Date: Authorised Signatory:

Place: Name of the Person:

Designation:

Firm Name & Seal:

13. Other Terms & Conditions for Bidder/MSP

13.1 General Conditions

13.1.1 In case the MSP is found in-breach of any condition(s) of bid or supply order, at any stage during the course of supply/ installation/commissioning or warranty period, the legal action as per rules/laws, shall be initiated against the MSP and EMD/PBG shall be forfeited.

13.1.2 Purchaser reserves the right to modify and amend any of the stipulated condition/criterion given in this bid, depending upon project priorities vis-à-vis urgent commitments. Purchaser also reserves the right to accept/reject a bid, to cancel/abort bid process and/or reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected agencies on the grounds of such action taken by the Purchaser.

13.1.3 Purchaser shall not be responsible for any misinterpretation or wrong assumption by the Bidder, while responding to this bid document.

13.1.4 The purchaser reserves the right to procure any quantity deemed appropriate based on the Bill of Material quoted by the Bidder during the entire course of the contract validity. Furthermore, the purchaser reserves the right to place Contracts as per the quantity required by Purchaser and may also utilize the same contract and unit rates for future procurement activities until the expiration of the contract's validity.

13.2 Labour Laws

13.2.1 The MSP shall, and hereby agrees to, comply with all the provisions of Indian Labour Laws and industrial laws in respect of the deployed resources.

13.3 Adherence to safety procedures, rules, regulations & restriction

13.3.1 MSP shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. Purchaser’s employee shall also comply with safety procedures/policy.

13.3.2 The Purchaser shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

13.3.3 Access to the Purchaser’s Data centre shall be strictly restricted in the following manner.

13.3.4 No access to any person except those explicitly authorised by the Purchaser shall be allowed entry. Even if granted, access shall be restricted to system/equipment necessary to run the engagement and access to any other equipment must be strictly precluded by necessary means, locks, video surveillance, etc.

13.3.5 No access to any employee of the Bidder, except the essential staff who has genuine work-related need, shall be furnished. All such access shall be logged in a loss-free manner for permanent record with unique biometric identification of the employee to avoid misrepresentations or mistakes.

13.4 Applicability of the IT Act and Rules

13.4.1 MSP shall ensure that offered solution as part of project scope and ensuing policies and procedures to have strict compliance to all cyber/information security policies, procedures and regulation and its subsequent updates issued by Government of India or its authorised agencies during the entire Project duration.

13.5 Information Security

13.5.1 The MSP shall not carry and/or transmit any material, information, layouts, diagrams, storage media or any other goods/material in physical or electronic form, which are proprietary to or owned by the Purchaser, out of premises without prior written permission from the Purchaser.

13.5.2 MSP acknowledges that Purchaser proprietary information or materials, whether developed by Purchaser or being used by Purchaser pursuant to a license Contract with a third party (the foregoing collectively referred to herein as “proprietary information”) are confidential and proprietary to Purchaser; and MSP agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorised use or disclosure thereof, which care shall not be less than that used by MSP to protect its own proprietary information. MSP recognizes that the goodwill of Purchaser depends, among other things, upon MSP keeping such proprietary information confidential and that unauthorised disclosure of the same by MSP could damage Purchaser and that by reason of MSP’s duties hereunder. MSP may come into possession of such proprietary information, even though MSP does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by the contract. MSP shall use such information only for the purpose of performing the said services.

13.5.3 MSP shall, upon termination of the Contract for any reason, or upon demand by Purchaser, whichever is earliest, return any and all information provided to MSP by Purchaser, including any copies or reproductions, both hardcopy and electronic. Any proprietary tools of the bidder, if any used for the project and MSP Pre-existing IPR will remain with the bidder.

13.5.4 The authorised signatory of the MSP shall sign the NDA with reference to this bid “The Official Secrets Act, 1923” within 7 days and submit the same along with the acceptance of the Contract letter.

13.5.5 All the deployed resources shall sign the NDA with reference to “The Official Secrets Act, 1923” within 7 days after confirmation of acceptance of the resource by Purchaser.

13.6 Official secrets

13.6.1 The Service Provider shall ensure and inform all persons employed by it in any works in connection with the Contract that the Official Secrets Act, 1923 shall apply and continue to apply to them even after execution and expiry of the Contract or resignation by any employee and that they shall be bound to not disclose any information regarding this Contract to any third party. The Service Provider shall bring to the notice of the Purchaser any information found to be leaked or disclosed. Where such leakage or disclosure is brought to the notice of the Purchaser or the Purchaser detects any leakage or disclosure during the Contract Period (including any period for which the Contract is extended) or after its expiry, the person concerned as well as the Service Provider shall be liable for penal action. The Purchaser shall have the liberty to terminate the Contract without notice, thereby invoking the exit management provisions of this Agreement.

13.7 Exit Management

13.7.1 The MSP shall submit a structured and detailed exit management plan post signing of the contract; the exit management plan shall be finalized by the MSP in consultation with the Purchaser.

13.7.2 The exit management requirements as elaborated below shall be read in conjunction to and in harmony with related clauses of the contract.

13.7.3 Given the critical nature of the service, it is imperative that a well-defined exit management strategy be made ready which shall enable easy transition of activities when the Contract expires/ is truncated.

13.7.4 Accordingly, the MSP shall submit an exit management plan within two months of Go-Live, which shall focus on the key activities it shall perform to ensure that a seamless transition of knowledge and activities be possible, and the same shall be evaluated. The exit management plan shall be based on the plan proposed by the MSP in its technical proposal. The final exit management plan shall have to be mutually agreed upon by Purchaser and the Bidder.

13.7.5 The MSP shall understand that ensuring a smooth transition at the end of the project period is a key requirement from Purchaser. The MSP needs to update the exit management plan on half yearly basis or earlier or whenever required by Purchaser in case of major changes during the entire Contract period. While proposing the exit management plan, the MSP shall ensure that the subsequent points are taken care of.

13.7.6 At the end of the Contract Period or during the Contract Period or Contract termination, if any other agency is identified or selected for providing services related to the scope of work as in the contract, the MSP shall ensure proper and satisfactory transition is made to the other agency. In case Purchaser wants to take over the project itself, then MSP has to ensure proper transition to the team designated by Purchaser.

13.7.7 All risks during transition stage shall be properly documented by MSP and mitigation measures be planned in advance and recorded in the exit management plan so as to ensure smooth transition without any service disruption.

13.7.8 The MSP shall provide all knowledge transfer of the system to the satisfaction of Purchaser as per the specified timelines.

13.7.9 The exit management period starts:

(a) In case of expiry of Contract, at least 12 Months prior to the date when the Contract comes to an end, or

(b) In case of termination of Contract, on the date when the notice of termination is sent to the Bidder.

13.7.10 The exit management period ends on the date agreed upon by the Purchaser or 12 Months after the beginning of the exit management period, whichever is earlier. In case of termination 12 Months exit period applies there also until Purchaser decides otherwise.

13.8 Transfer of Project documentation and data

13.8.1 Before the expiry of the exit management period, the MSP shall deliver relevant records and reports pertaining to the Project and its design, implementation, operation, and maintenance including all operation, maintenance records and manuals pertaining thereto and complete as on the divestment date.

13.8.2 The MSP shall provide the Purchaser with a complete and up to date list of the documents, data and relevant system details to be transferred to the Purchaser within 30 days of start of Exit Management Period.

13.8.3 The MSP shall pass on to the Purchaser, the subsisting rights in any licensed products on terms not less favourable to the Purchaser, than that enjoyed by the Bidder.

13.8.4 Even during the Exit Management period, the MSP shall continue to perform all their obligations and responsibilities as stipulated under the contract, and as may be proper and necessary to execute the Scope of Work in terms of the bid, to execute an effective transition and to maintain business continuity.

13.8.5 All solution provided by MSP under the scope of the bid shall be interoperable during the transfer/hand over at time of exit/Contract termination. No proprietary service is to be used or implement by the Bidder. Any customization, tools or effort required for smooth transfer of documentation and data arising out of interoperability issue shall be borne by the Bidder.

13.8.6 The MSP shall assist the Purchaser to migrate the current services from the current infrastructure to Purchaser.

13.8.7 All equipment and solution utilised to deliver the project scope shall have valid service Contract and shall not be under end of life during Contract period.

13.8.8 The MSP shall share the details of all existing service contracts and agreements executed with current vendors, Service Provider to Purchaser on yearly basis.

13.8.9 Upon exit or termination, the MSP shall hand over all hardware to NIC in proper working condition.

13.9 <u>Intellectual Property Rights</u>

13.9.1 Subject to the other provisions contained in this Clause, the MSP shall agree that all deliverables created or developed by the MSP, specifically for the Purchaser, together with any associated copyright and other intellectual property rights, shall be the sole and exclusive property of National Informatics Centre (Purchaser).

13.9.2 The Purchaser shall acknowledge that:

(a) In performing services under the Contract, the MSP may use its proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by the MSP prior to or independent of the services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the services hereunder, (“the MSP’s Pre-Existing IP”).

(b) Notwithstanding anything to the contrary contained in the Contract, the MSP shall continue to retain all the ownership, the rights title and interests on all the MSP’s Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the MSP from using the MSP’s Pre-Existing IP in any manner.

(c) If any of the MSP’s Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under the Contract, the MSP hereby grants to the User Department/Purchaser a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license of the deliverables with the right to sublicense through multiple tiers, to use, copy, install, perform, display, modify and create derivative works of any such deliverables and only as part of the deliverables in which they are incorporated or embedded.

(d) Purchaser being the owner of all the IPs created in the deliverables, except the Pre- Existing IPs of the MSP used in the development and deployment, shall have exclusive rights to use, copy, license, sell, transfer, share, deploy, develop, modify or any such act that the organisation/Purchaser may require or find necessary for its purpose. The IP rights of the Purchaser shall indefinitely subsist or continue in all future derivatives of the deliverables.

(e) The MSP or its deployed resources shall have no claims whatsoever on the deliverables and all the IPs created in deliverables except its Pre-Existing IPs for which it shall grant all authorizations to the organisation/Purchaser for use as detailed in the Clause (c) above.

(f) Except as specifically and to the extent permitted by the bidder, the organisation/Purchaser shall not engage in reverse compilation or in any other way arrive at or attempt to arrive at the source code of the bidder's Pre-Existing IP, or separate MSP's Pre-Existing IP from the deliverable in which they are incorporated for creating a standalone product for marketing to others.

(g) The organisation/Purchaser shall warrant that the materials provided by the organisation/Purchaser to MSP for use during development or deployment of the application shall be duly owned or licensed by the organisation/Purchaser.

(h) The Purchaser's contractual rights to use the Standard Software or element of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with relevant licence to a legally constituted successor organisation (e.g., a reorganisation of a public entity formally authorised by the government or through a merger acquisition of a private entity).

13.10 Publicity

13.10.1 The MSP shall not publicize any information pertaining to this Project or the Purchaser without seeking prior written consent of the Purchaser.

13.11 Warranty

13.11.1 The warranty of all supplied ZTNA solution shall start after the date of Go-Live.

13.11.2 The MSP warrants that all the Goods are new, unused, and of the most recent or current models, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the Contract.

13.11.3 The MSP further warrants that the Goods shall be free from defects arising from any act or omission of the Supplier or arising from design, materials, and workmanship, under normal use in the conditions prevailing in the country of final destination.

13.11.4 Unless otherwise specified in the Other terms and conditions, the warranty shall remain valid as indicated in Section 2, scope of work after the Goods, or any portion thereof as the case may be, have been deployed and accepted at the final destination indicated in Section 2, scope of work, after the date of shipment from the port or place of loading in the country of origin, whichever period concludes earlier.

13.11.5 Upon receipt of such notice, the MSP shall expeditiously repair or replace the defective Goods or parts thereof at no cost to the Purchaser.

13.11.6 If having been notified, the MSP fails to remedy the defect within the specified period, the Purchaser may proceed to take within a reasonable period such remedial action as may be necessary, at the MSP's risk and expense and without prejudice to any other rights which the Purchaser may have against the MSP under the Contract.

14. Events of Default by MSP

14.1 <u>Events of Default</u>

14.1.1 The failure on the part of the MSP to perform any of its obligations or comply with any of the terms of this Contract shall constitute an Event of Default on the part of the Bidder. The events of default as specified above may include inter-alia the following:

(a) The MSP has failed to perform any instructions or directives issued by the Purchaser which it deems proper and necessary to execute the scope of work under the Contract, OR

(b) The MSP/MSP's Team has failed to conform with any of the Service/Facility Specifications/standards as set out in the scope of work of this bid Document or has failed to adhere to any amended direction, modification or clarification as issued by the Purchaser during the term of this Contract and which the Purchaser deems proper and necessary for the execution of the scope of work under this Contract.

(c) The MSP has failed to demonstrate or sustain any representation or warranty made by it in this Contract, with respect to any of the terms of its Bid and this Contract.

(d) The MSP has failed to comply with or is in breach or contravention of any applicable laws of India.

14.1.2 Failure of the successful MSP to comply with the Bid requirements shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD/PBG. In case of exigency, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done shall be borne by the bidder.

14.2 <u>Compliance to Digital Personal Data Protection Act, 2023</u>

14.2.1 MSP shall ensure all the personal data is stored in compliance with Digital Personal Data Protection Act, 2023. The MSP shall also ensure that personal data is being encrypted at rest and in motion, or used in tokenised form, or obfuscated/masked; and the access privileges to the back-end data segment are limited to the minimum necessary set of authorised Users and are protected with multi-factor authentication.

14.2.2 **<u>Defects Liability Period</u>**:

(a) the MSP warrants that the Services have been delivered as per description, scope/ quantum, performance standards and quality outlined in the contract. This Defect Liability shall be in effect for a period stipulated in the contract (or if not specified for ninety (90) days) from completing the Services. The contract shall be deemed alive during this period, even if final payment and/ or Performance Guarantee has been released.

(b) During the Defects Liability Period, upon discovering any deficiencies in outputs/ outcomes attributable to a shortfall in scope/ quantum, performance standards and quality of the performed Services, the Purchaser shall give written notice to the bidder.

(c) Upon receiving such notice, the MSP shall, within 21 days (or within any other period, if stipulated in the contract), expeditiously remedy or reperform the Services or parts thereof, free of cost, at the site.

(d) If the Bidder, having been notified, fails to rectify/ replace the defect(s) within 21 days (or within any other period, if stipulated in the contract), it shall amount to breach of Contract, and the Purchaser shall proceed to take such remedial action(s) as deemed fit by it as detailed.

*********************END OF THE RFP DOCUMENT*********************