NOTICE INVITING TENDER FOR
TRUNKEY BASIS

For
Commissioning of Cyber Security Solutions for National Crime Records Bureau (NCRB)
Ref: ITI/2025-26/Def/Mktg/CSS

ITI LIMITED

(A Govt. of India Enterprise)
Defence-Marketing
ITI Limited,First Floor, Core 6,
Scope Complex, Lodi Road, New Delhi-110003
website: https://www.itiltd.in/
Email: skumar_bcdel@itiltd.co.in
CIN No: L32202KA1950GOI000640

1. Introduction.

ITI Limited, a Public Sector Undertaking under the Department of Telecommunications, Ministry of Communications, is a leading Telecom equipment manufacturer and solution provider in India. The major customers are BSNL, BBNL, MTNL, Defense, Paramilitary forces, Railways, Banks, Central & State Govt. departments, Institutions and research organizations like ISRO.

ITI Limited has been undertaking various projects in all fields of telecommunications and information technology and also continuously deploying new technologies in the field of Telecom, ICT, Networking, e-Governance etc. ITI has diversified its operation and has been executing projects in the field of Smart Infrastructure (Smart Cities, Safe Cities, Smart Energy Meters, Smart Classrooms, Smart Poles etc), Bharatnet etc. ITI has been executing projects in latest technologies like GPON, OLT, ONT, OFC, HDPE etc.

ITI Limited would like to address the tender on turnkey basis for selection of backend partner for Commissioning of cyber security solutions for National Crime Records Bureau (NCRB). In this connection ITI Limited, invites sealed tender from eligible bidders for addressing the above tender opportunity and implementing the project as per their scope of work finalized with ITI.

2. Important Dates.

Date of tender Upload	30-04-2026
Due Date for tender Submission	12-05-2026 up to 11:00 AM
Estimated Cost (Approx.)	**Rs.500000000/-**
Technical Specification	**As per mentioned in GeM Bid-** GEM/2026/B/7361141Dated: 24-04-2026
Pre Empanelment Queries/Pre Bid meeting	NO
ITI Contact Person	**Mr.Sandeep Kumar,** **DGM-Projects** **Ph.:011-24368533,24360555** **Email:**-skumar_bcdel@itiltd.co.in **https://www.itiltd.in** **Helpdesk:** **Mr.Faiz Ahmad Khan,** **AEE-Projects** **e-mail: faizahmad_nsu@itiltd.co.in**
Tender Fee	Rs. 5,000/-+ Rs. 900/- = Rs. 5,900/-(Non-Refundable)
Earnest Money Deposit (EMD)	**Rs.10000000/-**
PBG/Security Deposit/e-PBG	3%
Duration of e-PBG required (Months)	74
All other additional terms and Condition	**As mentioned in Bid document.**
The Bank Details of ITI Limited for NEFT/RTGS/Net Banking :	The Bank Details of ITI Limited for NEFT/RTGS/Net Banking is as below: Online RTGS/ NEFT

	Bank: State Bank Of India, Industrial Finance Branch, Residency Road, Bangalore-560025 MICR: 560002059 IFSC: SBIN0009077 A/C No.: 10637729843 EMD may also accepted in the form of BG
Mode of submission	Thru ITI e-tender portal https://itilimited.ewizard.in/.

3. Tender Scope of work & Technical compliance:-

As per Tender Reference/Bid Number: GEM/2026/B/7361141Dated: 24-04-2026 ITI inviting TENDER/BID for selection of backend partner for commissioning of cyber security solutions for National Crime Records Bureau (NCRB). The scope of this project encompasses the design, supply, deployment, integration, commissioning, and lifecycle support of a comprehensive Cyber Security Infrastructure for the National Crime Records Bureau (NCRB) and establish a fully functional, on-premises Security Operations Centre (SOC) and Network Operations Centre (NOC) to ensure 24x7x365 monitoring, detection, response, and management of all cybersecurity threats across NCRB's digital ecosystem.All the technical specification must compliance as per customer bid.

4**. Instruction to Bidders**

The bidders are required to submit soft copies of their bid electronically on the e-Wizard Portal using valid Digital Signature Certificates. Below mentioned instructions are meant to guide the bidders for registration on the e-Wizard Portal, prepare their bids in accordance with the requirements and submit their bids online on the e-Wizard Portal. For more information, bidders may visit the Portal (https://itilimited.ewizard.in/.).

a. REGISTRATION PROCESS ON ONLINE PORTAL:
Bidders to enroll on the e-Procurement module of the portal https://itilimited.ewizard.in/ by clicking on the link "Bidder Enrolment".

a) The bidders to choose a unique username and assign a password for their accounts. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. This would be used for any communication from the e-Wizard Portal.
b) Bidders to register upon enrolment, with their valid Digital Signature Certificate (Class III Certificates with signing and Encryption key) issued by any Certifying Authority recognized by CCA India with their profile.
c) Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse.
d) Bidder then logs in to the site through the secured log-in by entering their user ID/password and the password of the DSC / e-Token.
e) After registration send mail to Helpdesk: helpdeskeuniwizarde@gmail.com for Account activation.
f) As per portal norms Registration Fee will be applicable.

b. TENDER DOCUMENTS SEARCH:

a) Various built-in options are available in the e-Wizard Portal like Department name, Tender category, estimated value, Date, other keywords, etc. to search for a tender published on the Online Portal.

b) Once the bidders have selected the tenders they are interested in, they may download the required documents/tender schedules. These tenders can be moved to the respective 'Interested tenders' folder.

c) The bidder should make a note of the unique Tender No assigned to each tender, in case they want to obtain any clarification/help from the Helpdesk.

5. BID PREPARATION:

a) Bidder should take into account any corrigendum published on the tender document before submitting their bids.
b) Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.
c) Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that needs to be submitted. Any deviations from these may lead to rejection of the bid.
d) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document/schedule and generally, they can be in PDF/XLSX/PNG, etc. formats.

6. BID SUBMISSION:

a) Bidder to log into the site well in advance for bid submission so that he/she uploads the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
b) The bidder to digitally sign and upload the required bid documents one by one as indicated in the tender document.
c) Bidders to note that they should necessarily submit their financial bids in the prescribed format given by department and no other format is acceptable.
d) The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, the opening of bids, etc. The bidders should follow this time during bid submission.
e) All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data, which cannot be viewed by unauthorized persons until the time of bid opening.
f) The uploaded tender documents become readable only after the tender opening by the authorized bid openers.
g) Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.
h) The off-line tender shall not be accepted and no request in this regard will be entertained whatsoever.
i) As per portal norms Tender Processing Fee will be applicable.

7. AMENDMENT OF BID DOCUMENT:

At any time prior to the deadline for submission of proposals, the department reserve the right to add/modify/delete any portion of this document by the issuance of a Corrigendum, which would be published on the website and will also be made available to the all the Bidder who has been issued the tender document. The Corrigendum shall be binding on all bidders and will form part of the bid documents.

8. ASSISTANCE TO BIDDERS:

a) Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.
b) Any queries relating to the process of online bid submission or queries relating to e- Wizard Portal, in general, may be directed to the 24x7 e-Wizard Helpdesk. The contact number for the helpdesk is 8448288994/86/87/89/88/81/90/92/82 011-49606060, 07903269552, 9355030608, 9055030613, 7903810198,

9355030606, 9315620706, 9355030623, 9355030628, 8800526452, 9205898228, 9122643040, 9355030604, eprochelpdesk.01@gmail.com, eprochelpdesk.44@gmail.com, eprochelpdesk.06@gmail.com.

c) The tender inviting authority has the right to cancel this e-tender or extend the due date of receipt of the bid(s).
d) The bid should be submitted through e-Wizard portal (https://itilimited.ewizard.in/) only.
e) All payments should be done through e-Wizard Payment gateway.

5(i)	**EligibilityCriteriaofApplicants**	
	a	**CompanyProfile**: The Bidder shall be a Company incorporated /registered in India under Companies Act 1956/2013/ proprietorship/ partnership firm/ Limited Liability Partnership (LLP) and should be in operations continuously for at least 5 years as on the last date of submission of bid. 1) In case the bidder has executed any work/project with/for ITI in the last 5years, it is essential that a satisfactory certificate signed by at least DGM level/or above officer from ITI to be submitted for such project. 2) In case CMC followed by project execution, the CMC charges quoted by bidder are optional and ITI reserves the right to either award CMC to the bidder or float a separate tender at the end of project completion which will be abide by bidder. 3) Any financial liability (like contract processing fee, Agreement Stamp fee, Portal fee, BG making fee etc.) on ITI for this project will be borne by Bidder.
	b	a) Minimum average Turnover during each of the last three financial years (2022-23, 2023-24 and 2024-25), should be at least 2500 Lakh (s). b) Net Worth of the bidding entity during each of the last three financial years (2022-23, 2023-24 and 2024-25) should be in positive. c) The Bidder shall submit copy of Audited statements/CA certificate for last three years should be submitted along with technical proposal.
	c	**for selection of backend partner for commissioning of cyber security solutions for National Crime Records Bureau (NCRB). The scope of this project encompasses the design, supply, deployment, integration, commissioning, and lifecycle support of a comprehensive Cyber Security Infrastructure for the National Crime Records Bureau (NCRB) and establish a fully functional, on-premises Security Operations Centre (SOC) and Network Operations Centre (NOC) to ensure 24x7x365 monitoring, detection, response, and management of all cybersecurity threats across NCRB's digital ecosystem.**For more details refer to scope of work as per GeM BID Documents.
	d	The bidder should not have been blacklisted or debarred by any Pvt Ltd/State / Central Government or their agencies or Public Sector Undertakings (PSUs) as on bid submission date for corrupt, fraudulent or any other unethical business practices or for any other reason. Undertaking as per the format attached in **Annexure-I** duly signed by authorized signatory of bidder.
	e	All the applicable annexures and documents is as per customer BID.
	f	The supply item/OEM must be as per manufacturer certifications mentioned in BID. The technical specification of all the supplied items/ equipments as per the Operational characteristics and features as mentioned in bid **Appendix-B.** All the above sites/solution & technical specifications must be complied with the original GeM Tender.
	g	Undertaking for willingness to work with ITI as per customer tender etc. terms and conditions.
	h	EMD (Back to Back Basis): The bidder seeking EMD exemption, must submit the valid supporting document for the relevant

		category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. EMD & Performance security should be in favour of Beneficiary, wherever it is applicable.EMD of unsuccessful bidders should be returned back once the contract is finalized. The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. EMD & Performance security should be in favour of Beneficiary, wherever it is applicable.	
	i	Undertaking expressing willingness to sign agreement with ITI.	
	j	Bidder shall provide valid OEM Authorization Certificate for all the products quoted as well as certify that the proposed product is not declared end of sale. OEM documents and all applicable annexures/appendix shall be provided as per required by customer RFP	
	k	Consortium is not allowed. Bid splitting not applied. No part bidding allowed.	
	l	ITI reserve the right to reject /cancel the bid at any time without assigning any reason.	
	m	The agency should have successfully completed similar works(definition of similar Work should be clearly defined) during the last 3 Years ending last day of the month Previous to the one in Which bids are received as indicated below: i. Three similar completed works each costing not less than 20% Of the estimated cost of work. OR ii. Two similar completed works each costing not less than 25% of the estimated cost of work OR iii. One similar completed work costing not less than 40% of the estimated cost of work. **Similar Work:-**The bidder/OEM must have the experience in the same field as mention in work scope and technical specification.	
	n	Our company reserves the right that if any product, service or equipment is being manufactured in ITI limited , its supply and service must be provided to us by the vendor.	
5(ii)		**General : Provide Compliance for the following**	**YES/NO**
	a	All activities like Proof of concept on "No Cost No Commitment" (NCNC) basis wherever applicable will be the responsibility of bidders	
	b	Bidder should be willing to impart required training during undertaking services & execution of project (if applicable)	
	c	Bidder should be willing to sign an exclusive agreement with ITI for smooth execution of the project and all commercial terms will be as per the customer Tender/PO on back-to-back basis.	
	d	PBG will be taken from back-end partner, once ITI will be declared L1. Performance Bank Guarantee (PBG) required for the bid will be borne by the selected bidder.	
	e	LD Clause: LD shall be as per ITI Clauses (@ 0.5% of order value per week or part thereof subject to a maximum of 10% of the undelivered portion/ the order value (if the item(s) cannot be used unless full supply is made) or to cancel the order and purchase the materials from alternative source at the risk and cost of the supplier) OR as per the customer PO/tender clause whichever is higher.	

	f	Payment Terms: a) Payment terms will be as per back to back basis. b) Payment to the vendor shall be done after deduction of all i. LD/recoveries imposed by customer (if any) ii. ITI's margin	
	g	The bidder shall give an undertaking for the following: a. To extend end to end support of partnership b. To support ITI and bid in this tender with ITI as lead bidder c. To support ITI for preparation of the tender, post bid clarifications, technical presentations and any other requirements as per tender.	
	h	**Delivery Schedule:** Delivery Schedule as per the customer Bid/Tender/ PO on back-to-back basis.(if applicable)	
	i	**Consignee Details:** As per bid and if any changes will be provided after the award of the work	
	j	Bidder will be responsible for any shortcoming in the BOM and the same should be rectified free of cost	
	k	Bidder should not be insolvent (Self Declaration).	
	l	ITI reserve the right to reject or cancel the bid at any time without assigning any reason.	
5(iii)		**Checklist of documents/information to be submitted: (These documents shall be used for evaluating technical parameters for bidder qualification.)**	
	a	Company Profile	
	b	Certificate of Incorporation a per clause 5(i)(a)	
	c	Memorandum & Articles of Association	
	d	Audited financial statements for the last 3 years (FY 2022-23, 2023-24 & 2024-25).	
	e	GST Registration Certificate	
	f	Copy of PAN Card	
	g	CIN (Corporate Identity Number), if applicable	
	h	Any other relevant registration documents on registration with other appropriate authorities (ESI, EPFO, etc.)	
	i	Authorization letter in the company letterhead authorizing the person signing the bid for this tender and Power of Attorney (POA).	
	j	Undertaking in letter head to indemnify ITI from any claims / penalties / statutory charges, liquidated damages, with legal expenses etc.	
	k	Undertakings in Company letter head as per Annexure I.	
	l	Bidders Details as per Annexure II.	
	m	Clause by clause compliance of tender terms with references to supporting documents as per Annexure III.	

	n	Pre-Contract Integrity Pact as per Annexure-V a) "Bidders participating in the tender have to agree to sign Integrity Pact on placement of order / contract" b) "Those bidders who are not willing to sign Integrity Pact will not be considered for bid opening"
	o	The bidder should give an undertaking on the company's letterhead that all the documents/certificates/information submitted by them against this tender are genuine.
	p	Bidder shall submit technical data sheet by highlighting each complied specification. Wherever technical specifications and operational/functional requirements not mentioned in datasheet, OEM compliance shall be submitted.
	q	Work order / Contract clearly highlighting the scope of work, Bill of Material and value of the contract/order; and Completion / Commission Certificate issued & signed by the competent authority of the client entity on the entity's Letterhead.
	r	Complete tender and customer tender document duly signed and stamped on each page by the bidder be uploaded.
	s	Conditional bids will not be entertained and summarily rejected. Only online bids on https://itilimited.euniwizarde.inportal will be accepted and no physical bids will be accepted.
	t	**Average Annual Turnover** Average annual turnover over the last three financial years(FY 2022- 2023, FY 2023- 2024, FY 2024- 2025- (a) More than 200 Crores (b) More than 150 Crores but Less than/Equal to 200 Crores (c) More than 125 Crores but Less than/Equal to 150 Crores (d) Less than/Equal to 125 Crores
	u	**Manpower** Full time employees on payroll of bidder working in the business unit providing "IT/ITeS" services as on bid submission date.- a) More than 100(b) More than 50 but Less than/Equal to 100 (c) More than 25 but Less than/Equal to 50 (d) Less than /Equal to 25
	v	**Certifications**- ISO 9001,ISO 27001,ISO 14001, ISO 20000,ISO 45001,CMMi Level 3 or higher
	w	**Project Experience** -The Bidder should have completed projects in IT/ITeS including manpower with minimum value of INR 30 CR and above during last three (3) years as on bid submission date. (a) More than/Equal to 10 projects (b) Between 6-9 projects (c) Between 3-5 projects (d) Less than 3 projects , Work Order + Certificates of Completion (Certified by the Statutory Auditor/Company Secretary).
	x	**Technical Documentation (TD) -** TD for understanding of Current requirement as per scope of work, proposed service approach, methodology, work plan for performing the assignment etc. Details of proposed deployment plan, manpower retention strategies and handling of staff resignation including provision of a backup pool. • Detailed approach & methodology for providing technical support to the project, capacity building for resources and Escalation Matrix. • Proper readable Document submission as well as proper indexing.
	y	Bidder should have to submit detailed Approach and Methodology with Bid document.
5(iv)		**Financial Bid:**
		L1 Evaluation Method: A- Lump sum Quote for supply and service items as per Schedule of Requirements (SoR) and Scope of Work (SoW) in INR (without Taxes) B- Margin to ITI as a percentage of A C - Absolute value of Margin = A*B D- Overall Quoted price=A-C

		• Duringevaluationbidderswithleast“D”willbeconsideredasL1. • The bid having higher value of “B” will be selected in case of tied D. • If the bidder is selected, during the final tender submission, the price to be quoted shall not be more than price “A” and the margin offered to ITI shall not be less than “B” **SoR & SoW Was as per Tender document and all clarifications & Amendments/Corrigendum**

09. Special Conditions of tender:

a. No advance will be paid to the bidder, even though ITI is eligible to get advance from the customer being a front end bidder.
b. The selected bidder, who has partnered with ITI for a particular tender/ project shall not partner with any other lead bidder for the same tender/project
c. If the bidder is selected, during the final tender submission, the margin offered to ITI shall not be less than the quoted price.

10. Special Conditions of TENDER:

a. No advance will be paid to the bidder, even though ITI is eligible to get advance from the customer being a front end bidder.
b. The selected bidder, who has partnered with ITI for a particular tender/ project shall not partner with any other lead bidder for the same tender/project
c. If the bidder is selected, during the final tender submission, the margin offered to ITI shall not be less than the quoted price.
d. The estimated project amount stated in this document is provisional and subject to revision during the actual bidding process. Consequently, the bidder's quoted amount may also fluctuate (increase or decrease).
e. The work order for the actual RFP will be awarded based on the ratio of the bidder's quoted amount to the revised estimated project value, as compared to the initial estimated value stated in this document."
f. The requisite final solution to all the supplied equipments/Services must be end to end support till final solution as per RFP clause.

11. Other Terms and conditions:

Confidentiality

a) All documents, drawings, samples, data, associated correspondence or other information furnished by or on behalf of the Procuring Entity to the contractor, in connection with the contract, whether such information has been furnished before, during or following completion or termination of the contract are confidential.
b) If advised by the Procuring Entity, all copies of such information in original shall be returned on completion of the contractor’s performance and obligations under this contract.

12. Transparency

All procuring authorities are responsible and accountable to ensure transparency, fairness, equality, competition and appeal rights. This involves simultaneous, symmetric and unrestricted dissemination of information to all likely bidders, sufficient for them to know and understand the availability of bidding opportunities and actual

means, processes and time limits prescribed for completion of registration of bidders, bidding, evaluation, grievance redressal, award and management of contracts.
It implies that such officers must ensure that there is consistency, predictability, clarity, openness, equal opportunities in processes.

13. Fall Clause:

Fall clause is a price safety mechanism in rate contracts. The fall clause provides that if the rate contract holder reduces its price or sells or even offers to sell the rate contracted goods or services following conditions of sale similar to those of the rate contract, at a price lower than the rate contract price, to any person or organization during the currency of the rate contract, the rate contract price will be automatically reduced with effect from that date for all the subsequent supplies under the rate contract and the rate contract amended accordingly.

The provisions of fall clause will however not apply to the following:

i. Export/Deemed Export by the supplier;
ii. Sale of goods or services as original equipment prices lower than the price charged for normal replacement;
iii. Sale of goods such as drugs, which have expiry date;
iv. Sale of goods or services at lower price on or after the date of completion of sale/placement of order of goods or services by the authority concerned, under the existing or previous Rate Contracts as also under any previous contracts entered into with the Central or State Government Departments including new undertakings (excluding joint sector companies and or private parties) and bodies.

14. Price Variation

A suitable price variation formula should also be provided in the tender documents, to calculate the price variation between the base level and scheduled delivery date.

15. Risk Purchase

If the empanelled partner fails to adhere to the quality norms, delivery schedules and other terms and conditions contained in this Tender after acceptance of purchase order and if no agreement is reached on the revised delivery schedule maximum up to 15 Business Days, then buyer shall have the liberty to procure the material from an alternate source at the Empanelled partner's risk and cost, and the Empanelled partner shall be liable to make good the loss incurred by Buyer in this process

16. Indemnity:

The empanelled partner to indemnify ITI from any claims / penalties / statuary charges, liquidated damages, with legal expenses etc as charged by the customer. LD/ Penalties incurred on account of delay in supply, product failure during warranty if any and deficiency in Warranty and AMC services attributable to the partner shall be borne by the partner All terms and conditions of the customer tender/PO will be applicable to the empanelled partner on back to back bass without affecting the margin of ITI.

17. Arbitration:
Any dispute arising out of this TENDER shall be settled and resolved by any such Authorized person appointed by Chairman and Managing Director of ITI Limited.

18. Set Off:
Any Sum of money due and payable to the supplier under this contract may be appropriated by the purchaser or any other person contracting through the ITI and set off the same against any claim of the purchaser for payment of a sum of money arising out of this contract or under any other contract made by the supplier with the purchaser.

19. The interested partner may like to discuss the customer tender related information, TENDER Bidding Conditions, Bidding Process and clarifications, if any with the Deputy General Manager-Marketing

20. Intellectual Property Rights:

i. All deliverable, outputs, plans, drawings, specifications, designs, reports and other documents and software submitted by the contractor under this contract shall become and remain the property of the procuring entity and subject to laws of copyright and must not be shared with third parties or reproduced, whether in whole or part, without: the procuring entity's prior written consent.
ii. The contractor shall, not later than upon termination or expiration of this contract, deliver all such documents and software to the procuring entity, together with a detailed inventory thereof.
iii. The contractor may retain a copy of such documents and software but shall not use it for any commercial purpose.

21. Language of offers:
The offers prepared by the Company and all the correspondences and documents relating to the offers exchanged by the companies shall be written in English language.

22. In the event that ITI is required to provide demonstration or working of the product to their buyers, the same shall be arranged by the bidder selected partner/OEM at latter's cost and expenditure.

23. Cost of TENDER:

The bidder shall bear all costs associated with the preparation and submission of his offer against this TENDER, including cost of presentation for the purposes of clarification of the offer, if so desired by ITI. ITI will, in no case be responsible or liable for those costs, regardless of the conduct or outcome of the TENDER process.

24. **Purchaser's Right to accept any bid and to reject any or All Bids or to cancel the TENDER:**
ITI Limited reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids, at any time prior to award of contract without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds of purchaser's action.

25. Amendment of TENDER:
At any time prior to the last date for receipt of offers, ITI, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the TENDER document by an amendment. In order to provide prospective bidder reasonable time in which to take the amendment into account in preparing their offers, ITI may, at their discretion, extend the last date for the receipt of offers and/or make other changes in the requirements set out in the Invitation for TENDER.

26. **Disclaimer:**
ITI and/or its officers, employees disclaim all liability from any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of ITI and/or any of its officers, employees.

27. Accessibility of TENDER Document:
Complete Tender document with terms and conditions is provided in the following websites

(i) http://www.itiltd.in
(ii) https://itilimited.euniwizarde.in

(iii) http://eprocure.gov.in

Annexure-I

Undertakings (To be in Bidder's Letter Head)

M/s .....do here by undertake the following

1. Are not blacklisted by Central Govt./ any State or UP Govt/ PSU/ organized sector in India
2. To work with ITI as per this TENDER and Customer Tender terms and conditions. Also, we agree to implement the project (scope of work as per Tender terms and conditions including investment) covering Warranty& post-warranty services, maintenance etc, in the event of ITI winning the contract on back-to-back basis.
3. To submit Security Deposit of 5% per transaction to customer/ITI (as decided by ITI),
4. that we will be equipped with the required manpower with qualifications, certifications and experience as mentioned in the customer tender.
5. to get required certificate& support (warranty & post-warranty/maintenance) in the name of ITI from the OEM as per customer tender requirement.
6. To obtain relevant statutory licenses for operational activities.
7. to sign MoU/Teaming Agreement, Integrity Pact with ITI for addressing the customer tender as per customer's tender terms and conditions.
8. to indemnify ITI from any claims / penalties/ statuary charges, liquidated damages, with legal expenses etc as charged by the customer.
9. to support the offered equipment for a minimum period of 10 years including warranty and AMC or as per customer tender conditions.
10. To supply equipment/components which conform to the latest year of manufacture.
11. The bidder should give certificate stating that all the hardware/ software supplied under the contract shall not contain any embedded malicious codes that could inhibit the desired functions of the equipment or cause the network to malfunction in any manner.

Annexure-II

Bidders Profile

1.	Name and address of the company			
2.	Contact Details of the Bidder (Contact person name with designation, Telephone Number, FAX, E- mail and Web site)			
3.	Area of the business			
4.	Annual Turnover for financial years (Rs in Cr)	2022-23	2023-24	2024-25
5.	IT Turnover for 3 financial years (Rs in Cr)	2022-23	2023-24	2024-25
6.	Positive Net Worth as on 31.03.2025			
7.	Date of Incorporation,			
8.	GST Registration number			
9.	PAN Number			
10.	CIN Number, if applicable			
11.	Number of manpower in company's rolls			
12	Work Experience details: **Annexure IV**			
13.	Certifications details like ISO or any other certification as per requirements of Customer.			

Annexure-III

Compliance Statement

Sl. No.	**Clause No.**	**Clause**	**Compliance (Complied/Not Complied)**	**Remarks with Documentary Reference**

Annexure- IV

Project Experience

Sl. No.	Name of project	Value	Name of customer	Attached Documentary Proof

Annexure - V

INTEGRITY PACT

TENDER No.

THIS Integrity Pact is made on……day of ..... 2025.

BETWEEN:

ITI Limited having its Registered & Corporate Office at ITI Bhavan, Dooravaninagar, Bangalore – 560 016 and established under the Ministry of Communications, Government of India (hereinafter called the Principal), which term shall unless excluded by or isrepugnant to the context, be deemed to include its Chairman & Managing Director, Directors, Officers or any of them specified by the Chairman & Managing Director in this behalf and shall also include its successors and assigns) ON THE ONE PART

AND:
…….. represented by
Chief Executive Officer (hereinafter called the Contractor(s), which term shall unless excluded by or is repugnant to the context be deemed to include its heirs, representatives, successors and assigns of the contractor ON THE SECOND PART.

Preamble:

WHEREAS the Principal intends to award, under laid down organizational procedures, contract for ……. of ITI Limited. The Principal, values full compliance with all relevant laws of the land, regulations, economic use of resources and of fairness/ transparency in its relations with its Contractor(s).

In order to achieve these goals, the Principal has appointed an Independent External Monitor (IEM), who will **monitor** the tender process and the execution of the contract for compliance with the principles as mentioned herein this agreement.

WHEREAS, to meet the purpose aforesaid, both the parties have agreed to enter into this Integrity Pact the terms and conditions of which shall also be read as integral part and parcel of the Tender Documents and contract between the parties.

NOW THEREFORE, IN CONSIDERATION OF MUTUAL COVENANTS STIPULATED IN THIS PACT THE PARTIES HEREBY AGREE AS FOLLOWS AND THIS PACT WITHNESSETH AS UNDER:

SECTION 1 – COMMITMENTS OF THE PRINCIPAL

The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:

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

b. The Principal will, during the TENDER process treat all bidder(s) with equity and reason. The Principal will in particular, before and during the TENDER process, provide to all bidder(s) the same information and will not provide to any bidder(s) confidential/ additional information through

which the bidder(s) could obtain an advantage in relation to the TENDER process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons. If the principal obtains information on the conduct of any of its employee, which is a criminal offence under IPC/PC Actor if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary action as per its internal laid down Rules/ Regulations.

SECTION 2 – COMMITMENTS OF THE BIDDER / CONTRACTOR

2.1 The Bidder(s)/Contractor(s) commits himself to take all measures necessary to prevent corruption. He commits himself observe the following principles during the participation in the TENDER process and during the execution of the contract.

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

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

c. The bidder(s)/contractor(s) will not commit any offence under IPC/PC Act, further the bidder(s)/contractor(s) will not use improperly, for purposes of competition of personal gain, or pass onto others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractor(s) of foreign original shall disclose the name and address of the Agents /representatives in India, if any. Similarly, the Bidder(s)/Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.

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

f. The Bidder(s)/Contractor(s) will not bring any outside influence and Govt bodies directly or indirectly on the bidding process in furtherance to his bid.

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

SECTION 3 – DISQUALIFICATION FROM TENDER PROCESS & EXCLUSION FROM FUTURE CONTRACTS

If the Bidder(s)/Contractor(s), during TENDER process or before the award of the contract or during

execution has committed a transgression in violation of Section 2, above or in any other form such as to put his reliability or credibility in question the Principal is entitled to disqualify Bidder(s)/Contractor(s) from the TENDER process.

If the Bidder(s)/Contractor(s), has committed a transgression through a violation of Section 2 of the above, such as to put his reliability or credibility into question, the Principal shall be entitled exclude including blacklisting for future TENDER/contract award process. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the Principal taking into consideration the full facts and circumstances of each case, particularly taking into account the number of transgression, the position of the transgressor within the company hierarchy of the Bidder(s)/Contractor(s) and the amount of the damage. The exclusion will be imposed for a period of minimum one year.

The Bidder(s)/Contractor(s) with its free consent and without any influence agrees and undertakes to respect and uphold the Principal's absolute right to resort to and impose such exclusion and further accepts and undertakes not to challenge or question such exclusion on any ground including the lack if any hearing before the decision to resort to such exclusion is taken. The undertaking is given freely and after obtaining independent legal advice.

A transgression is considered to have occurred if the Principal after due consideration of the available evidence concludes that based on facts available there are no material doubts.

The decision of the Principal to the effect that breach of the provisions of this Integrity Pact has been committed by the Bidder@)/ Contractor(s) shall be final and binding on the Bidder(sj/ Contractor(s), however the Bidder(s)/Contractor(8) can approach IEM(s) appointed for the purpose of this Pact.

On occurrence of any sanctions/ disqualifications etc arising out from violation of integrity pact Bidder(s)/ Contractor(s) shall not entitled for any compensation on this account.

Subject to full satisfaction of the Principal, the exclusion of the Bidder(s)/Contractor(s) could be revoked by the Principal if the Bidder ($)/ Contractor(s) can prove that he has restored/ recouped the damage caused by him and has installed a suitable corruption preventative system in his organization.

SECTION 4 – PREVIOUS TRANSGRESSION

4.1 The Bidder(s)/ Contractor(s) declares that no previous transgression occurred in the last 3 years immediately before signing of this Integrity Pact with any other company in any country conforming to the anti-corruption/ transparency International (TI) approach or with any other Public Sector Enterprises/ Undertaking in India of any Government Department in India that could justify his exclusion from the TENDER process.

4.2 If the Bidder(s)/ Contractor(s) makes incorrect statement on this subject, he can be disqualified from the TENDER process or action for his exclusion can be taken as mentioned under Section-3 of the above for transgressions of Section-2 of the above and shall be liable for compensation for damages as per Section- 5 of this Pact.

SECTION 5 – COMPENSATION FOR DAMAGE

5.1 If the Principal has disqualified the Bidder(s)/Contractor(s) from the TENDER process prior to the award according to Section 3 the Principal is entitled to forfeit the Earnest Money Deposit/Bid Security/ or demand and recover the damages equitant to Earnest Money Deposit/Bid Security apart

from any other legal that may have accrued to the Principal.

5.2 In addition to 5.1 above the Principal shall be entitled to take recourse to the relevant provision of the contract related to termination of Contract due to Contractor default. In such case, the Principal shall be entitled to forfeit the Performance Bank Guarantee of the Contractor or demand and recover liquidate and all damages as per the provisions of the contract agreement against termination.

SECTION 6 – EQUAL TREATEMENT OF ALL BIDDERS/CONTRACTORS

6.1 The Principal will enter into Integrity Pact on all identical terms with all bidders and contractors for identical cases.

6.2 The Bidder(s)/Contractor(s) undertakes to get this Pact signed by its subcontractor(s)/sub-empanelled partner(s)/ associate(s), if spy, and to submit the same to the Principal along with the TENDER document/contract before signing the contract. The Bidder(s)/Contractor(s) shall be responsible for any violation(s) of the provisions laid down in the Integrity Pact Agreement by any of its subcontractors/ sub-empanelled partners / associates.

6.3 The Principal will disqualify from the TENDER process all bidders who do not sign this Integrity Pact or violate its provisions.

SECTION 7 – CRIMINAL CHARGES AGAINST VIOLATIG BIDDER(S)/CONTRACTORS

7.1 If the Principal receives any information of conduct of a Bidder(s)/Contractor(s) or sub-contractor/ sub-empanelled partner/associates of the Bidder(s)/Contractor(s) which constitutes corruption or if the principal has substantive suspicion in this regard, the principal will inform the same to the Chief Vigilance Officer of the Principal for appropriate action.

SECTION 8 – INDEPENDENT EXTERNAL MONITOR(S)

8.1 The Principal appoints competent and credible Independent External Monitor(s) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extend the parties comply with the obligations under this pact.

Details of IEM appointed by ITI are as under:

Name: ShriAtul Jindal IFS (Retd.),
Independent External Monitor (IEM)
Address- 3/10 VisheshKhand Opp. Little Friend School Gomti Nagar,
Lucknow-226010(UP)
E-mail:` atulindia1947@gmail.com

IEM – II
Shri Benny John, IRS (Retd.),
Villa No. 36, Kent Plam Villas,
Fort Valley Township, Athani,
Kakkanad, Ernakulam,
Kerala – 682 030

8.2 The Monitor is not subject to any instructions by the representatives of the parties and performs his functions neutrally and independently. He will report to the Chairman and Managing Director of the Principal.

8.3 The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all product documentation of the Principal including that provided by the Bidder(s)/Contractor(s). The Bidder(s)/Contractor(s) will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The Monitor is under contractual obligation to treat the information and documents Bidder(s)/Contractor(s) with confidentiality.

8.4 The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the project provided such meeting could have an impact on the contractual relations between the Principal and the Bidder(s)/Contractor(s). As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in specific manner, refrain from action or tolerate action.

8.5 The Monitor will submit a written report to the Chairman & Managing Director of the Principal within …….. to ……..Weeks from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.

8.6 If the Monitor has reported to the Chairman & Managing Director of the Principal a substantiated suspicion of an offence under relevant IPC/PC Act, and the Chairman & Managing Director of the principal has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

8.7 The word 'Monitor' would include both singular and plural.

SECTION 9 - FACILITATION OF INVESTIGATION

9.1 In case of any allegation of violation of any provisions of this Pact or payment of commission, the Principal or its agencies shall be entitled to examine all the documents including the Books of Accounts of the Bidder(s)/Contractor(s) and the Bidder(s)/Contractor(s) shall provide necessary information and documents in English and shall extend all help to the Principal for the purpose of verification of the documents.

SECTION 10 - LAW AND JURISDICTION

1.1 The Pact is subject to the Law as applicable in Indian Territory. The place of performance and jurisdiction shall the seat of the Principal.

1.2 The actions stipulated in this Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extent law in force relating to any civil or criminal proceedings.

SECTION 11 – PACT DURATION

This Pact begins when both the parties have legally signed it. It expires after 1 year on completion of the warranty/ guarantee period of the project /work awarded, to the fullest satisfaction of the Principal.

If the Bidder(s)/Contractor(s) is unsuccessful, the Pact will automatically become invalid after three months on evidence of failure on the part of the Bidder(s)/Contractor(s).

If any claim is lodged/made during the validity of the Pact, the same shall be binding and continue to be valid despite the lapse of the Pact unless it is discharged/determined by the Chairman and Managing Director of the Principal.

SECTION 12 - OTHER PROVISIONS

12.1 This pact is subject to Indian Law, place of performance and jurisdiction is the Registered & Corporate office of the Principal at Bengaluru.

12.2 Changes and supplements as well as termination notices need to be made in writing by both the parties. Side agreements have not been made.

12.3 If the Bidder(s)/Contractor(s) or a partnership, the pact must be signed by all consortium members and partners.

12.4 Should one or several provisions of this pact turn out to be invalid, the remainder of this pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions

12.3 Any disputes/ difference arising between the parties with regard to term of this Pact, any action taken by the Principal in accordance with interpretation thereof shall not be subject to any Arbitration.

12.4 The action stipulates in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

In witness whereof the parties have signed and executed this Pact at the place date first done mentioned in the presence of the witnesses:

For PRINCIPAL For BIDDER(S)/CONTRACTOR(S)

…… ……

Name Designation Name Designation

Witness

1. …….. 1. ……..

2. …….. 2. . ……

TECHNICAL PROPOSAL

For

COMMISSIONING OF CYBER SECURITY SOLUTIONS for

NATIONAL CRIME RECORDS BUREAU (NCRB)

NATIONAL CRIME RECORDS BUREAU (NCRB)

1. SCOPE OF THE PROJECT

The scope of this project encompasses the **design, supply, deployment, integration, commissioning, and lifecycle support of a comprehensive Cyber Security Infrastructure** for the National Crime Records Bureau (NCRB) and establish a fully functional, on-premises **Security Operations Centre (SOC)** and **Network Operations Centre (NOC)** to ensure 24x7x365 monitoring, detection, response, and management of all cybersecurity threats across NCRB's digital ecosystem.

The key deliverables under the project include the following but are not limited to:

- Deployment of **advanced perimeter and endpoint security solutions**, including Next Generation Firewalls (NGFW).
- Implementation of **centralized Security Information and Event Management (SIEM)** and **Security Orchestration, Automation and Response (SOAR)** platforms.
- Establishment of **high availability SOC and NOC infrastructure** with associated management terminals, monitoring dashboards, and secure connectivity.
- Integration of **Data Loss Prevention (DLP) and Network Access Control (NAC)** to secure sensitive data and applications.
- Conduct of **Vulnerability Assessment and Penetration Testing (VAPT)** as per CERT-In.
- **Deployment of trained cybersecurity personnel (L1, L2, L3 analysts)** for continuous operations and threat resolution.
- Implement an **end-to-end, fully integrated cybersecurity solution** adhering to the security hardening and compliance protocols.
- Design and implement **in-depth network architecture in line with National Critical Information Infrastructure Protection Centre (NCIIPC) and CIS guidelines other like MHA etc,** including multi-layer network security and complete segregation as per NCRB policies.
- Execute **VM migration from existing infrastructure to the new environment**, as mutually agreed.
- Design and create **Golden Images for Linux OS** to ensure standardized and secure VM deployments for all future virtual infrastructure requirements.
- **Design & implement on premises patch Management Solution** along with necessary hardware & software. The solution would support diversified platform viz. windows, macOS, Linux patching (agent-based or agentless) & also support > 250 popular third-party apps (viz. Adobe, Java, Chrome, Firefox etc.)
- Provision for deployment a high-performance **server virtualization cluster (Hypervisor-based)** with redundancy, performance tuning, and continuous uptime.
- Implement **centralized data backup** solution using Backup with a **minimum of one-year data retention**, supporting compliance with national cybersecurity and forensic investigation policies.
- Provision of **user training, documentation, warranty, and technical support** services.
- **Compliance with all applicable Government of India cybersecurity guidelines** at the time of Setup (CERT-In, NIC, MHA, NCIIPC etc.) and ISO 27001 best practices.

This project will enable NCRB to build a **resilient, proactive, and scalable cybersecurity infrastructure**, ensuring the protection of critical crime data and operational continuity in the face of evolving cyber threats.

2. EXISTING SYSTEM OVERVIEW

SL. NO	DESCRIPTION	QNTY
1.	DESKTOPS (All Outdated, All between 5-10 Years Old)	340 (Approx..)
2.	SERVERS Existing Servers-49 (All Outdated, more than 5 years Old), 12 Servers To be Replaced with mutual consent	49
3.	L2/L3 SWITCHES	23
4.	FIREWALLS	4
5.	ROUTERS	4
6.	NETWORK CONVERTER	2
7.	STORAGE	9
8.	PDU	2

The complete IT Infrastructure which will be replaced with new IT Infrastructure (except HDD, SSD, NVME, SAS and other disk) will be offered for buyback including all but not limited to above BOQ's. All Buy back's list will be prepared on Mutual Consent with NCRB. This will be as per the E-Waste (Management) Rules, 2022. Vendor will provide the certificate after e-waste disposal as per the rule.

3. NEED FOR THE CYBER SECURITY SOLUTIONS

In an era where data is the most valuable asset, safeguarding national crime and law enforcement records is of paramount importance. The National Crime Records Bureau (NCRB), being the central repository of criminal data, biometric databases, and national-level crime analytics, is a **high-value target for sophisticated cyber threats** ranging from ransomware to state-sponsored attacks.

Given the growing complexity of NCRB's IT infrastructure, combined with increasing inter-agency data sharing, legacy system exposure, and rising cyber risk vectors, the need for a **holistic and future-ready cyber security framework** is both urgent and indispensable.

Key drivers for implementing this cyber security solution include:

- **Protection of Critical Information Infrastructure (CII):** NCRB applications are designated as critical by the Government of India and require real-time threat monitoring, isolation, and remediation capabilities to prevent any compromise of sensitive data.
- **Evolving Threat Landscape:** Modern cyberattacks bypass traditional defences using AI-driven exploits, zero-day vulnerabilities, and multi-stage intrusions that demand proactive and intelligent cyber defence mechanisms.
- **End-of-Life Legacy Components:** Many of NCRB's existing systems have outdated firmware and unsupported components, leaving exploitable gaps that necessitate upgradation to advanced security controls.
- **Regulatory Compliance:** Strict adherence to CERT-In, NIC, MHA, NCIIPC etc. guidelines is essential to maintain compliance and operational authorization in handling law enforcement data.
- **Public Trust and National Security:** Any cyber incident can undermine the trust in digital law enforcement mechanisms, disrupt services, and impact national security operations.

Implementing an integrated and intelligent cyber security solution will empower NCRB with **robust defence, continuous monitoring, rapid response, and future scalability**, ensuring a secure and resilient cyber environment for years to come.

4. OVERVIEW OF THE REQUIRED SOLUTION

A **comprehensive, modular, and defence-in-depth cyber security solution** is required which is tailored to the unique operational and security needs of the National Crime Records Bureau (NCRB). Our approach ensures protection across all layers—network, application, endpoint, and data—while enabling **real-time monitoring, automated incident response, and policy compliance** through a fully integrated Security Operations Centre (SOC) and Network Operations Centre (NOC).

The core objective of the solution will be to establish a **resilient cyber defence architecture** that not only prevents and detects threats but also responds intelligently to security incidents, ensuring **business continuity, data integrity, and regulatory adherence**.

Key highlights of the required solution must include the following (but not limited to):

- **Next-Generation Firewalls (NGFW):** For deep-packet inspection, application control, and intrusion prevention.
- **Security Information and Event Management (SIEM):** For centralized log correlation, threat analysis, and alerting.
- **Security Orchestration, Automation and Response (SOAR):** To enable automated response workflows, reduce incident response time, and ensure compliance.
- **Network Access Control (NAC):** Ensuring only authorized and policy-compliant devices access the NCRB network.
- **Data Loss Prevention (DLP):** Safeguarding sensitive crime and citizen data from unauthorized exfiltration.
- **SOC & NOC Setup:** With dedicated dashboards, and skilled resources for 24x7x365 operations.
- **High Availability Architecture:** All critical components will be configured in active-standby mode to eliminate single points of failure.
- **Compliance & Governance:** Designed in accordance with CERT-In, NIC, NCIIPC along with others like MHA guidelines etc.

The solution should be **scalable, standards-compliant, and tailored for mission-critical government deployments**, ensuring NCRB's infrastructure remains protected, agile, and future-ready.

A. EGDE FIREWALL

As part of NCRB's **multi-layered cyber-defence architecture**, a high-performance **Next-Generation Firewall (NGFW)** will be deployed at the **network perimeter**, serving as the **first line of defence against external threats**. To ensure **high availability (HA)** and **business continuity**, the NGFW will be deployed in an **active-active HA pair**, delivering **seamless failover** and **uninterrupted protection**.

In alignment with NCRB requirements, **Virtual Routing and Forwarding (VRF)** will be configured either on the firewall or the core switch, depending on design and operational needs. Additionally, **SNMP (Simple Network Management Protocol)** will be enabled across all network devices for **centralized monitoring, alerting, and compliance** with NCRB standards.

1.1 Key Capabilities of the NGFW

The NGFW consolidates **advanced security controls** into a unified platform, delivering deep visibility, granular control, and real-time threat mitigation:

1. **Stateful & Deep Packet Inspection (DPI):**
   Monitors connection states and inspects traffic across all OSI layers, detecting anomalies and blocking malicious activity in real time.
2. **Application Awareness & Control:**
   Identifies applications (including evasive or encrypted traffic) and enforces **granular usage policies**, regardless of port, protocol, or evasive techniques.
3. **Intrusion Prevention System (IPS):**
   Leverages **signature-based, heuristic, and behaviour-based detection** to block exploits, including zero-day attacks, while integrating with **real-time global threat intelligence feeds**.
4. **Advanced DNS Security:**
   Detects and blocks DNS tunnelling, command-and-control callbacks, and phishing by inspecting DNS queries and enforcing response policy zones.
5. **URL & Web Filtering:**
   Enforces browsing restrictions using **category-based filtering, reputation scoring, and custom allow/deny lists**.
6. **SSL/TLS Inspection:**
   Performs decryption and inspection of encrypted traffic to uncover hidden threats, with support for **certificate pinning, selective decryption policies, and compliance exclusions**.
7. **Malware Protection & Sandboxing:**
   Suspicious files are redirected to isolated **sandbox environments** for advanced analysis, ensuring detection of **polymorphic malware, ransomware, and targeted attacks**.
8. **DoS/DDoS Mitigation & IP Reputation Blocking:**
   Protects against volumetric, protocol, and application-layer floods while automatically **blocking IPs based on global reputation feeds**.

9. **Centralized Logging & SIEM Integration:**
   Forwards logs, flow data, and security alerts to the **enterprise SIEM** for **real-time monitoring, incident correlation, and forensic analysis**.

1.2 Advanced Policy Controls

The NGFW will enforce **fine-grained policies** to align with NCRB security directives, including:

- **Application Category Filtering** – differentiation between business and non-business applications.
- **IP-based Security Policies** – source/destination-based traffic control.
- **Geo-tagging & Location-based Filtering** – allowing or restricting connections by country or region.
- **Integration with NCIIPC Threat Feeds** – supporting **hash-based blocking (MD5/SHA256), custom IP ranges, individual IP addresses, and domain name filtering** for proactive and automated protection.
- **Custom Threat-Mitigation Rules** – enforcement of NCRB-specific security guidelines and sectoral compliance requirements.

1.3 Outcome

By deploying this **HA-configured NGFW solution** with **VRF-enabled segmentation, NCIIPC threat feed integration, and SNMP-based centralized monitoring**, NCRB will achieve a **robust, adaptive, and future-ready perimeter security posture**.

This architecture will:

- Prevent **unauthorized access** at the network edge.
- Detect and block **Advanced Persistent Threats (APTs)**.
- Mitigate **malware, ransomware, and zero-day campaigns**.
- Integrate with **NCIIPC intelligence feeds** for **hash, IP, and domain-based blocking**.
- Ensure **uninterrupted protection** through **redundancy and high availability**.
- Provide **full visibility and centralized policy enforcement** across the perimeter.

Ultimately, this deployment ensures that all incoming and outgoing traffic is comprehensively inspected, controlled, and threat-intelligence enriched—delivering NCRB a resilient and future-proof perimeter defence.

B. INTERNAL NEXT GEN FIREWALL

To safeguard NCRB's critical internal assets against sophisticated, multi-vector attacks, a dedicated **Next-Generation Firewall (NGFW)** will be deployed in an **active-active High-Availability (HA)** pair. Unlike the edge NGFW, the internal NGFW will be sourced from a **different OEM**, thereby enhancing **supply-chain resilience** and **technology diversity**.

Strategically positioned at the **core of the internal network fabric**, this Internal NGFW ensures that all traffic—**east-west** and **north-south**—between segmented security zones undergoes **full Layer 2–7 inspection** and policy enforcement. No inter-zone communication will bypass inspection, effectively minimizing **lateral threat movement**.

1.1 Architectural Highlights & Traffic Flow

• Micro-Segmentation & Zone Enforcement

Each security zone (User LAN, Server LAN, Management, DMZ, Development, DB Zone, Backup, etc.) is explicitly defined in the NGFW policy engine. Every traffic flow is classified as: source zone → destination zone → application → user → risk profile → hash/IP/domain This allows for highly granular inspection, matched against tailored **allow/deny rules**, including integration of **NCIIPC-supported hash values**, **individual/custom IP ranges**, and **monitored domain names**.

• Centralized Policy Orchestration

Zone-based security policies are authored once and synchronized across all HA peers (edge and internal), ensuring **uniform enforcement** and preventing **policy drift**—even across different firewall OEM platforms.

• Post-Inspection Connectivity

All **intra- and inter-zone traffic**, including **VLAN-tagged**, **VPN**, and **routed flows**, is inspected through the NGFW. Only traffic explicitly permitted by policy—including vetted hashes, IP ranges, and domains—is allowed, effectively reducing the **risk of lateral threat propagation**.

1.2 Core NGFW Capabilities

The Internal NGFW consolidates multiple advanced security functions into a single high-performance platform:

- **Deep Packet Inspection (DPI):** Full Layer 2–7 traffic analysis to detect anomalies, evasions, and embedded threats.
- **Intrusion Prevention System (IPS):** Signature- and behaviour-based detection for zero-day threats and unauthorized lateral movement, continuously updated with global and local threat feeds.
- **Application & User-Aware Access Control:** Enforces least-privilege access using user identity, group, device posture, and **application context**, independent of port/protocol.
- **SSL/TLS Decryption & Inspection:** Selective decryption of encrypted traffic for threat analysis; includes exclusions for **certificate-pinned and regulated applications**.

- **Advanced Malware Protection & Sandboxing:** Files are dynamically analysed in isolated environments using **multi-vector techniques** including hash matching with **NCIIPC threat indicators**.
- **URL / Domain Filtering:** Real-time classification and **reputation-based filtering** of web traffic; **specific domain names** can be allowed or blocked per policy.
- **Custom IP & Hash Blocking:** Security policies can reference **NCIIPC-published malicious file hashes**, **custom-defined IP address ranges**, and **specific IPs** to block or monitor.
- **DoS / DDoS Mitigation:** Real-time traffic analysis to detect and respond to floods using **rate limiting**, **challenge-response**, and **traffic shaping**.
- **IP Reputation & Threat Intelligence:** Integrates feeds from global sources and **NCIIPC**, enabling **real-time blacklisting** of known malicious IPs, TOR nodes, botnets, and C2 infrastructures.
- **API Integration & Automation:** RESTful APIs support dynamic policy updates, **real-time ingestion of IOCs (Indicators of Compromise)** from NCIIPC, and orchestration with SDN or automation frameworks.
- **Proxy Services:** Granular control and optimization of HTTP/HTTPS/FTP traffic using **full proxy**, including **content caching and normalization**.
- **High Throughput & SSL Offload:** Hardware-accelerated decryption and inspection capabilities maintain multi-Gbps performance with **low latency**.

1.3 SOC, SIEM & SOAR Integration

The Internal NGFW will feed real-time logs, alerts, and telemetry to NCRB's **SOC, SIEM, and SOAR** platforms, enabling:

- **Continuous Threat Visibility:** Full correlation of NGFW data with endpoint, identity, cloud, and external threat intelligence (including NCIIPC feeds) for **unified situational awareness**.
- **Adaptive Security Policies:** Dynamic quarantine of compromised hosts, domains, or hash-matched malware files through **automated policy enforcement**.
- **Accelerated Incident Response:** SOAR playbooks can invoke **automated response actions** such as isolating endpoints, denying traffic from flagged IPs, revoking credentials, or triggering sandbox analysis.

1.4 Strategic Advantage

By deploying **heterogeneous NGFWs** at the edge and internal layers—each optimized for its respective role—under a unified, API-driven policy framework, NCRB achieves:

- **Technology and OEM diversity**, increasing resilience to supply-chain and software risks.
- **End-to-end visibility and enforcement** across east-west and north-south network flows.
- **Dynamic, threat-intelligence-driven protection**, seamlessly integrating with **NCIIPC indicators**, hash databases, IP/domain blacklists, and behavioural signatures.

This architecture ensures that every transaction within NCRB's internal network is rigorously **validated**, **inspected**, and **controlled**, thereby establishing a **future-proof, adaptive defence posture** aligned with **national cybersecurity mandates and best practices**.

C. SIEM

An advanced **Security Information and Event Management (SIEM)** solution is required to serve as the central nervous system of NCRB's cyber defence framework. The SIEM platform will **aggregate, normalize, and correlate logs and events** from across the NCRB's IT ecosystem—including **firewalls, endpoints, servers, applications, and network devices**.

Key capabilities of the proposed SIEM include (but are not limited to):

- **Real-time threat detection** and **incident correlation** using behavioural analytics and threat intelligence.
- **Centralized log collection and retention** compliant with **CERT-In standards**, ensuring all logs are **stored securely for a minimum of one year**.
- **Customizable dashboards** and **alerting mechanisms** for enhanced **SOC visibility**.
- **Scalability** to handle high event volumes (≥10,000 EPS peak), ensuring performance under load.
- **Forensic analysis** and **compliance reporting** to support audit readiness and investigation workflows.
- **Ingestion of all logs from network and server devices** into the SIEM, ensuring comprehensive visibility and monitoring.
- **Tight integration with SOAR, NGFW, and NAC** components to enable end-to-end threat visibility, faster incident response, and improved security posture across NCRB's digital infrastructure, including logs from **NCRB infrastructure hosted at NIC cloud (CII systems)**.

1.1 Log Collection Server

As a foundational component of the SIEM architecture, a robust **Log Collection Server** is required to **securely gather logs** from all critical assets across the NCRB network—such as **firewalls, servers, switches, endpoints, and applications**.

Key features (but not limited to):

- Real-time log ingestion from distributed sources using **standard protocols** (Syslog, SNMP, APIs, etc.).
- High-throughput data processing to support **scalable event rates (EPS)**.
- **Secure transmission** and **encrypted storage** to maintain data integrity and confidentiality.
- **Built-in redundancy** and **failover mechanisms** to ensure continuous availability.
- **Pre-processing and normalization** for seamless integration with the correlation engine.
- Ingestion of **all network and server device logs** to ensure comprehensive coverage.

1.2 Log Management Server

The **Log Management Server** serves as the **centralized repository** for secure, long-term storage and efficient management of all log data collected from NCRB's IT infrastructure.

Key features (but not limited to):

- Centralized log aggregation from diverse sources—network devices, security appliances, servers, and endpoints.
- **Indexed, searchable storage** enabling rapid retrieval for **audit, investigation, and compliance**.
- **Retention policy enforcement** aligned with CERT-In guidelines, with **logs stored for a minimum of one year** for forensic traceability.
- **Compression and deduplication** for optimized storage utilization.
- **Tamper-proof architecture** to maintain the **integrity and authenticity** of all logs.

1.3 Log Correlation Server

The **Log Correlation Server** is the **intelligence core** of the SIEM ecosystem, designed to analyze, correlate, and prioritize security events across NCRB's network in real time. By applying **rule-based** and **behavioural analytics**, the server transforms raw log data into actionable security insights.

Key features (but not limited to):

- **Multi-source correlation** of logs from firewalls, endpoints, servers, and applications to detect patterns and anomalies.
- **Custom rule engine** for defining threat detection logic tailored to NCRB's risk profile.
- **Real-time alerting** and **risk scoring** for faster incident detection and prioritization.
- **Dashboards and reporting tools** for SOC analysts to visualize threat chains and event timelines.
- **Integration with SOAR** for **automated incident response** and **case management**.

D. SOAR

A powerful **SOAR platform** is required to enhance NCRB's cyber threat response capabilities through **orchestration, automation, and structured case management**. Seamlessly integrated with the SIEM, the SOAR system will empower security analysts to respond to threats with greater speed, accuracy, and consistency.

Key features should include the following (but not limited to):

- **Automated playbooks** to streamline incident investigation, containment, and escalation workflows.
- **Integration with threat intelligence feeds, firewalls, and NAC** for unified action across security tools.
- **Case management interface** for tracking, assigning, and documenting incident resolution.

- **Customizable response workflows** to reduce response time and analyst fatigue.
- **Audit trails and compliance reporting** for accountability and traceability.

The SOAR solution will enable NCRB to move from manual, reactive response to **automated, intelligence-driven security operations**, significantly improving operational efficiency and resilience.

1.1 Security orchestration

As a key pillar of cyber defence strategy for NCRB, **Security Orchestration** facilitates seamless integration and coordination across multiple security tools and systems. By creating a unified command layer, orchestration enables faster decision-making, improved visibility, and synchronized incident handling across the SOC environment.

Key capabilities include the following (but not limited to):

- **Centralized integration of diverse security tools**—SIEM, NGFW, threat intelligence, NAC, and more.
- **Automated data enrichment and threat context sharing** across systems in real time.
- **Streamlined workflows** for detection, triage, and escalation of incidents.
- **Reduced operational silos**, enabling analysts to operate through a unified console.
- **API-based connectivity** with both on-premises and cloud-native security platforms.

This orchestration layer ensures that NCRB's security posture is **coordinated, adaptive, and highly responsive**, reducing manual overhead and enabling proactive threat mitigation.

1.2 Security automation

Robust **Security Automation** reduces manual effort, accelerate incident response, and ensure consistent execution of security tasks across NCRB's digital infrastructure.

Key capabilities include the following (but not limited to):

- **Automated threat detection and response workflows** based on predefined playbooks.
- **Real-time alert triage**, enrichment, and prioritization to eliminate false positives.
- **Scripted actions** for tasks such as IP blocking, user isolation, or malware containment.
- **Integration with SIEM, and firewalls** for instant, coordinated defensive actions.
- **Continuous policy enforcement** and automated compliance checks.

By minimizing human intervention in repetitive tasks, security automation ensures **rapid, accurate, and scalable defence operations**, enabling NCRB's SOC team to focus on high-priority threats and strategic analysis.

1.3 Security response

A structured and intelligent **Security Response** mechanism designed to swiftly contain, mitigate, and recover from security incidents is required.

Key features should include the following (but not limited to):

- **Centralized incident dashboard** for real-time monitoring, classification, and escalation of security events.
- **Automated and manual response workflows** for threat isolation, policy enforcement, and recovery actions.
- **Collaboration tools** for SOC analysts to coordinate investigations and document incident lifecycle.
- **Root cause analysis and post-incident reporting** to strengthen defences against future threats.
- **Audit-ready logs and response records** to ensure transparency and compliance with regulatory mandates.

This unified response approach ensures NCRB can **rapidly neutralize threats, minimize impact, and maintain operational continuity**, all while supporting governance and compliance requirements.

E. NMS

A robust and scalable **Network Management System (NMS)** is required to enable centralized, real-time monitoring and management of NCRB's critical network infrastructure. The NMS will provide complete visibility into the performance, health, and utilization of all network components.

Key Features should include the following (but not limited to):

- **Auto-discovery of network devices** with topology visualization
- **SNMP-based health and availability monitoring** of routers, switches, and firewalls
- **Proactive fault detection and alerting** to minimize downtime
- **Bandwidth and traffic analytics** for efficient capacity planning
- **Role-based dashboards and reporting** to support NOC operations

The NMS will be fully integrated with the proposed SOC/NOC ecosystem, allowing NCRB to maintain **high network availability, rapid fault response, and optimal performance** across its secure communication environment.

F. NAC

An advanced Network Access Control (NAC) solution is required to ensure only authorized, authenticated, and policy-compliant devices can access NCRB's critical network infrastructure.

Key features should include the following (but not limited to):

- **Device authentication and profiling** to identify, classify, and control access for users and endpoints.
- **Policy-based access control** enforcing security posture compliance before network admission.
- **Guest and contractor access management** through dynamic VLAN assignment and limited access zones.
- **Real-time monitoring and remediation** for non-compliant devices or anomalous behaviour.
- **Integration with SIEM** for contextual response and threat isolation.
- **NAC combined with AAA (Authentication, Authorization, and Accounting)** forms a critical foundation for implementing **Zero Trust Network Access (ZTNA)** by ensuring identity verification, policy enforcement, and activity logging for every user and device attempting to access the network.

By implementing NAC, NCRB can achieve complete visibility, dynamic control, and zero-trust enforcement across its network, significantly enhancing its cybersecurity defence posture.

G. DLP

A robust **Data Leakage Prevention (DLP)** solution is required to safeguard NCRB's sensitive and classified information from unauthorized access, accidental exposure, or intentional exfiltration.

Key features should include the following (but not limited to):

- **Content-aware inspection** to detect and block sensitive data such as criminal records, PII, and classified reports.
- **Real-time monitoring of data in motion, at rest, and in use**, across endpoints, emails, and network channels.
- **Policy-driven controls** to prevent unauthorized sharing, printing, or copying of sensitive information.
- **Automated alerts and response actions** for data breach attempts.
- **Comprehensive logging and reporting** for forensic investigation and compliance audits.

With DLP in place, NCRB will ensure **data confidentiality, regulatory compliance, and operational integrity**, reinforcing trust in its digital infrastructure.

H. SOC

Establishment of a state-of-the-art **Security Operational Centre (SOC)** at NCRB premises is required to enable **24x7x365 real-time threat monitoring, analysis, and response** across its entire digital infrastructure.

Key features should include the following (but not limited to):

- **Centralized visibility** through SIEM and SOAR integration for continuous security event correlation and automated incident response.
- **Tiered analyst setup (L1/L2/L3)** to handle threat detection, investigation, and escalation efficiently.
- **Log retention and forensic capabilities** as per CERT-In guidelines.
- **High availability and disaster recovery mechanisms** to ensure uninterrupted SOC operations.

This SOC will act as the **nerve center of NCRB's cyber defence ecosystem**, ensuring proactive risk mitigation, rapid response to incidents, and sustained cyber resilience. The entire SOC/NOC setup should have the minimum baseline capabilities specified in Annexure 'C'. The listed requirements are indicative and not exhaustive. Final requirements will be decided based on consent of NCRB management.

I. NETWORK OPERATION CENTRE (NOC):

A fully equipped **Network Operational Centre (NOC)** at NCRB headquarters is required to ensure continuous **monitoring, management, and optimization of the organization's critical network infrastructure**.

Key features of the proposed NOC should include the following (but not limited to):

- **Real-time monitoring of network devices**, bandwidth, and performance metrics using a centralized NMS dashboard.
- **Proactive detection of outages, bottlenecks, and configuration anomalies** to ensure high network availability.
- **Deployment of skilled L1/L2/L3 network engineers** for 24x7 operations, incident resolution, and escalation management.
- **Integrated alerting system** linked with SOC for coordinated threat and fault response.
- **Comprehensive reporting and trend analysis** for capacity planning and network health audits.

This NOC will serve as the **backbone of NCRB's IT operations**, ensuring resilient, secure, and uninterrupted connectivity across its digital ecosystem. The entire SOC/NOC setup should have the minimum baseline capabilities specified in Annexure 'C'. The listed requirements are indicative and not exhaustive. Final requirements will be decided based on consent of NCRB management.

i. EXISTING ARCHITECTURE

Existing logical architecture of NCRB network is as shown in below figure:

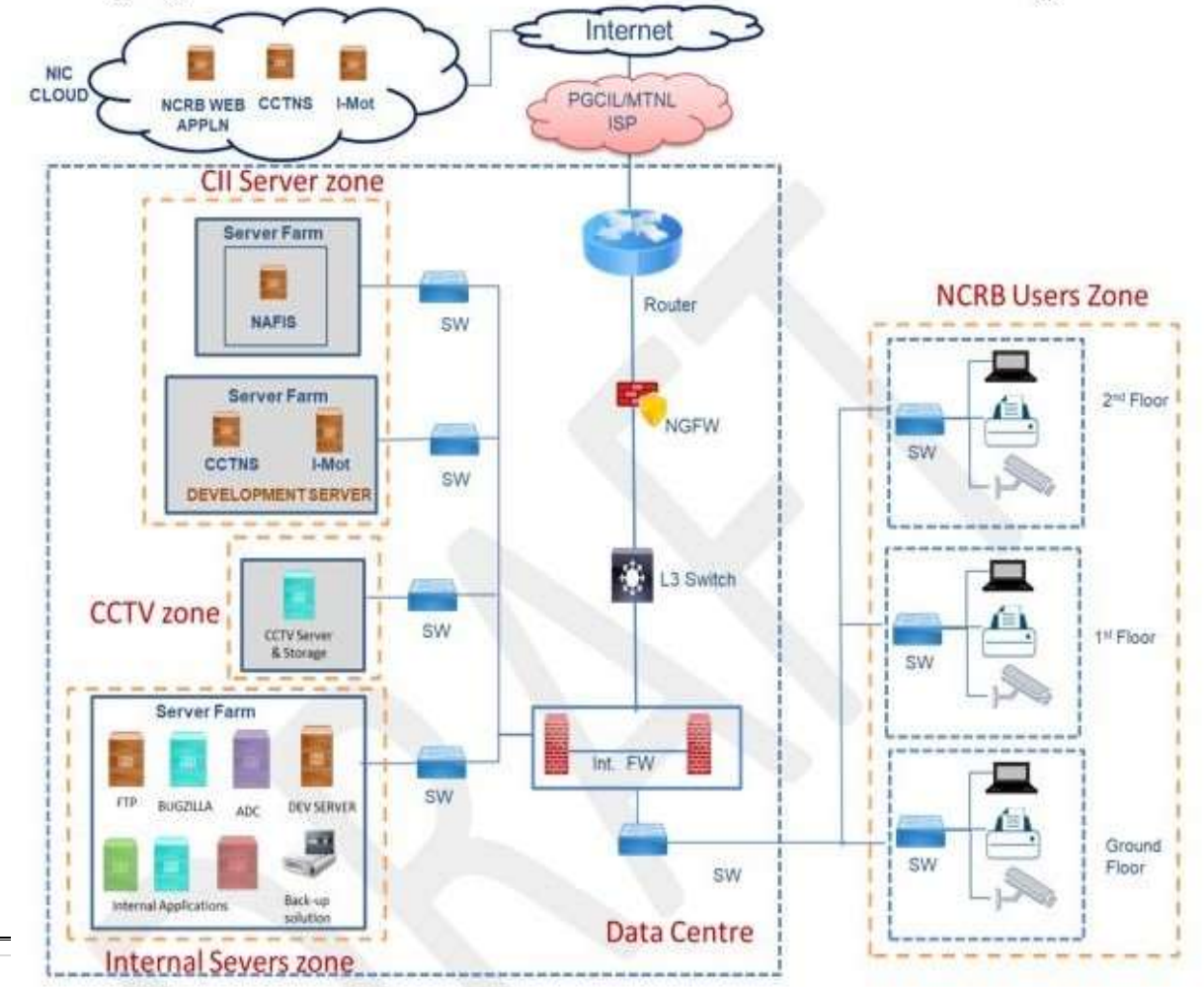
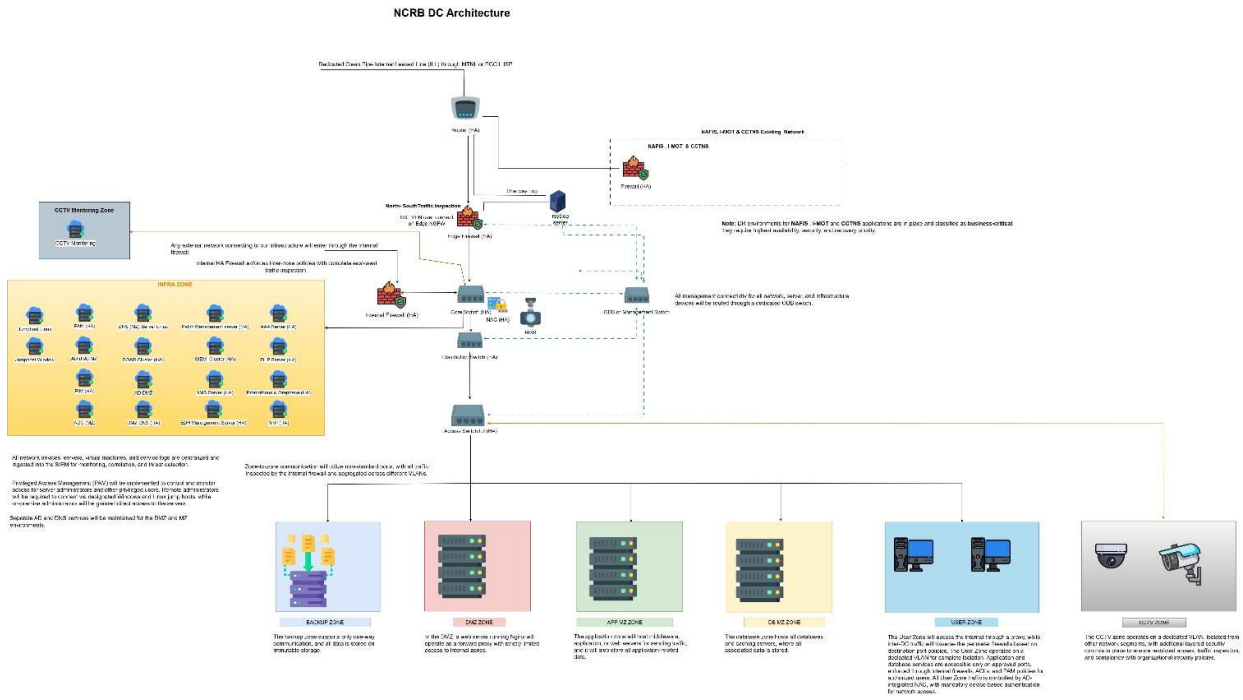


Figure 1: Existing Logical connectivity of NCRB Network

ii. PROPOSED ARCHITECTURE WITH IMPLEMENTATION OF NOC & SOC.*



***Ref Architecture is attached separately along with this proposal.**

iii. Key Points for Proposed Architecture.

Logging & monitoring

All network and security logs—from firewalls, NAC, and all other infrastructure devices (excluding user PCs)—are forwarded to the central SIEM, enabling comprehensive incident detection, real-time monitoring, and audit-ready reporting across the environment. All devices are time-synchronized via redundant NTP and use secure collectors/relay nodes for log delivery.

Segmentation & inter-zone control

The network is built on dedicated VLANs to ensure complete traffic isolation, secure segmentation, and strictly controlled inter-zone communication. Each functional zone (DMZ, Application, Database, Backup, and User) resides in its own VLAN to:

- Minimize lateral movement
- Simplify traffic management and routing
- Enforce inter-zone firewall policies with explicit allow-lists (standard ports only)

Remote Access- VPN

The edge/internet firewall provides Remote Access VPN for authorized users. Support users connecting via VPN land only on secured Linux or Windows Jump Hosts for administrative

access, while standard user traffic is directed to their respective PCs. All internet-bound user traffic passes through the proxy with NAT applied at the edge firewall.

Identity, directory, and service isolation
Separate DNS and Active Directory (AD) services are maintained for the DMZ and the internal (MZ) network, ensuring critical services remain isolated from public-facing components. All servers in the server zones are AD domain-joined and obtain network access only after NAC authentication.

Inter-DC security controls
Inter-DC traffic is strictly governed using destination-port allow-lists, ACLs, and Privileged Access Management (PAM)-based policies, ensuring only authorized and fully audited communications occur between server zones.

Zero Trust posture
Zero Trust Network Access (ZTNA) enforces identity-centric, least-privilege access for users and workloads, reducing reliance on perimeter-only security. Internal services apply mutual authentication and certificate management through the organization's PKI.

Hardening & compliance
OS hardening of all servers follows customer-approved SOPs and compliance baselines, with continuous configuration monitoring.

Traffic enforcement & inspection
A high-availability internal firewall enforces inter-zone policies and performs comprehensive east-west inspection. Where required, a port-channel is configured to the core, and VLAN sub-interfaces on the firewall are mapped 1:1 to security zones to ensure:

- Proper traffic segregation between VLANs
- Consistent zone-based policy enforcement
- Full visibility and inspection of east-west traffic

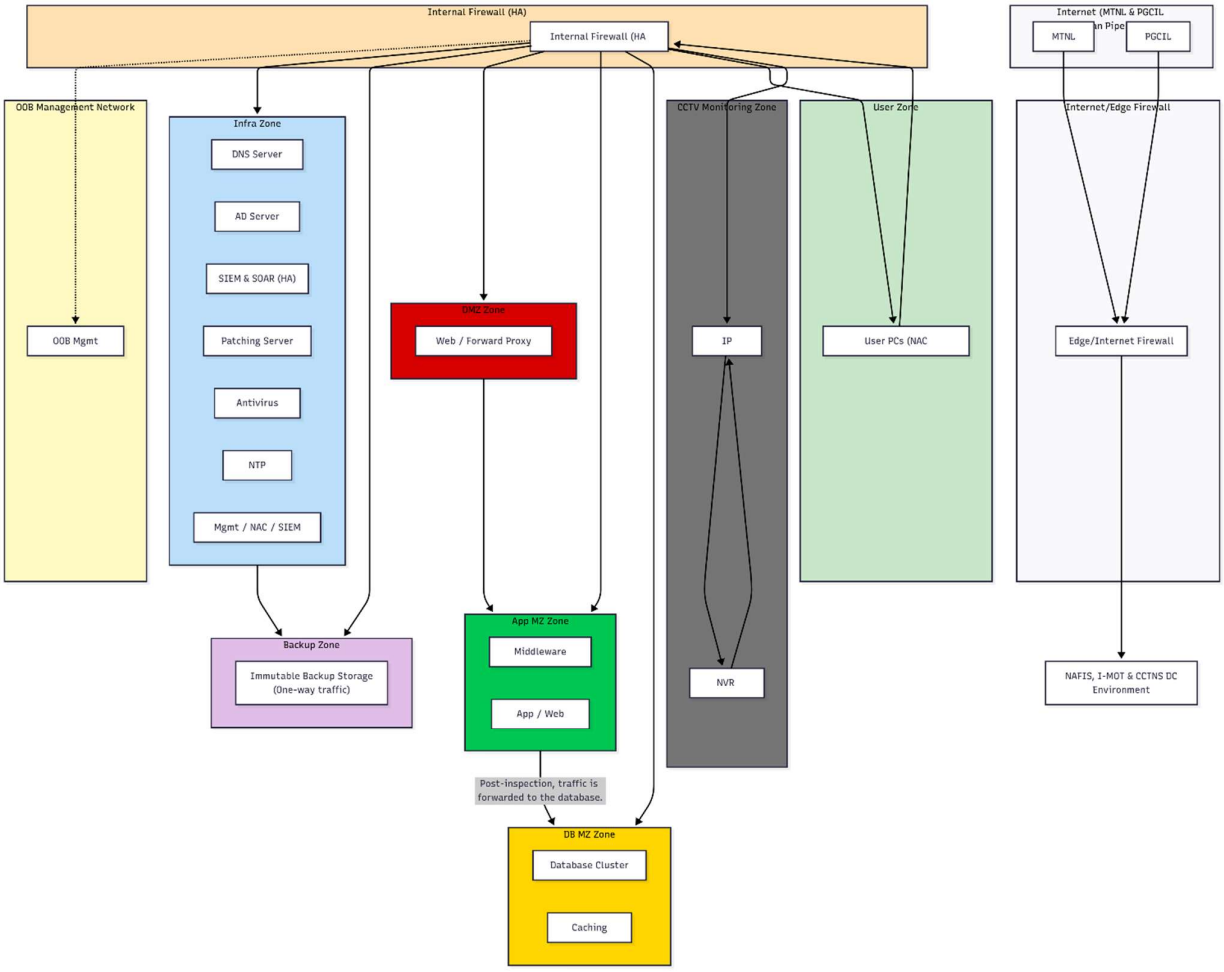
Outcomes

- Minimized broadcast domains and reduced attack surface
- Optimized network performance and deterministic routing
- Prevention of unauthorized lateral movement
- Alignment with Zero Trust principles
- Clear separation of duties between public and internal resources

Note (DR Priority)

DR environments for NAFIS I-MOT and CCTNS applications are in place and classified as business-critical. They require the highest priority in terms of availability, security, and disaster recovery readiness.

iv. TRAFFIC FLOW*



*Ref Traffic Flow is attached separately along with this proposal.

v. Traffic Flow Overview

a. Core Architectural Principles

- **Centralized Observability** – All zones log to SIEM (TLS syslog/agent); NTP-synced for event correlation.
- **Strict Zone Segmentation** – VLANs map 1:1 to security zones (DMZ, App MZ, DB MZ, Backup, User, CCTV, Mgmt, OOB); inter-zone flows via explicit firewall policies only.
- **Controlled Remote Access** – Admin ingress via RA-VPN → Mgmt VLAN Jump Host → target; NAT egress centralized at Edge FW.
- **Service Tier Isolation** – DMZ has standalone DNS/AD; NAC validation required before server joins internal domain.
- **Zero-Trust Enforcement** – Identity-based policy (AD groups) + PKI for mutual service authentication.
- **Full East–West Inspection** – Internal HA FW enforces L3–L7 policy between all zones.

b. **North–South Flows**

(*Traffic crossing between your internal network and the Internet*)

c. **User Browsing → Internet**

- **Purpose:** All user HTTP/HTTPS traffic is forced through the proxy for filtering, malware scanning, and logging before exiting to the internet.
- **Security rationale:**
  - **802.1X/NAC:** Ensures only authorized devices are on the User VLAN.
  - **AD-based rules:** Users get web access only if their account is authorized.
  - **SSL inspection:** Decrypts and inspects HTTPS to block threats hidden in encrypted traffic.
  - **Centralized NAT at Edge FW:** Keeps egress IP mapping consistent for auditing.
  - **Logging:** Both proxy and firewall logs feed SIEM for correlation.

d. **Public Access → DMZ Web**

- **Purpose:** External users access public-facing services (websites, portals) hosted in the DMZ.
- **Security rationale:**
  - **Edge FW VIPs:** Publish only specific IPs/ports to the public internet.
  - **IPS/DDoS:** Edge FW mitigates volumetric or protocol-based attacks.

e. **East–West Flows**

(*Traffic between internal security zones*)

DMZ → App MZ

- **Purpose:** DMZ web servers call application servers in the App MZ for business logic.
- **Security rationale:**
  - **App-specific ports only:** Prevents generic access; e.g., only 443, 8443 as required.
  - **mTLS (PKI):** Both sides authenticate with certificates, preventing impersonation.
  - **L7 inspection:** Detects anomalies in application requests.

f. **App MZ → DB MZ**

- **Purpose:** Applications query database servers for data.
- **Security rationale:**
  - **DB ports only:** Locks down to the database service protocol (e.g., 5432, 3306, 1433).
  - **TLS encryption:** Protects data in transit.
  - **East–west inspection:** Catches abnormal queries or data exfiltration attempts.

g. Servers → Backup VLAN (one-way)

- **Purpose:** Protect backups from ransomware or accidental deletion.
- **Security rationale:**
    - **Outbound-only rules:** Servers can send data to backup, but backup systems cannot initiate connections back.
    - **Protocol restriction:** Limits to backup-related traffic (e.g., NFS, SMB, HTTPS).
    - **Immutable storage:** Backup systems are configured to retain data unmodified.

h. Management / Services Flows

i. Remote Administration

- **Purpose:** Secure remote management of infrastructure.
- **Security rationale:**
    - **RA-VPN:** All remote admin traffic enters through encrypted VPN on Edge FW.
    - **Jump Host:** Single controlled entry point in Mgmt. VLAN — reduces exposure.
    - **No split-tunnel:** All traffic routes through corporate security stack.
    - **PAM/JIT:** Privileged credentials are granted temporarily and sessions are recorded.

J. OOB MANAGEMENT (OUT-OF-BAND MANAGEMENT)

- **Purpose:** Manage network and server hardware independently of production network.
- **Security rationale:**
    - **Physically/logically isolated:** Prevents production compromise from affecting OOB control.
    - **ACL restricted:** Only authorized jump/admin systems can connect.

a. Core Enterprise Services

- **DNS:** Internal zones use corporate DNS; DMZ uses a separate resolver for public-facing services to avoid leaking internal records.
- **AD/Kerberos:** Provides centralized identity and authentication; flows restricted to required ports and roles.
- **NTP:** Synchronizes device clocks for log correlation and incident analysis.
- **Patch/AV:** Updates are fetched by internal patch/AV servers, which use proxy for internet access — keeps endpoints off the internet directly.

b. Log Ingestion

- **Purpose:** Centralize monitoring and security alerting.
- **Security rationale:**

- **TLS syslog/agents:** Protects log integrity and confidentiality in transit.
- **Per-zone collectors:** Minimize cross-zone log traffic; improves resilience.
- **SIEM correlation:** Enables cross-device event analysis.

c. Inter-DC / Agency Flows

- **Purpose:** Secure connectivity to other law-enforcement networks (NAFIS, CCTNS).
- **Security rationale:**
  - **Destination port allow-lists:** Reduces risk by only opening exact business-required ports.
  - **PAM for admin flows:** Tracks and controls privileged access between environments.
  - **L7 inspection:** Detects malicious payloads or protocol misuse across WAN links.

Condensed Firewall Policy Matrix

S.No	From → To	Allowed Ports	Purpose
1	User → Proxy	3128/8080/443	Web via proxy
2	Proxy → Internet	80/443	Controlled egress
3	Internet → DMZ Web	80/443	Public access via WAF
4	DMZ → App	App ports	Web→ App tier
5	App → DB	DB ports	App→ DB
6	Servers → Backup	Backup proto	One-way backup
7	RA-VPN → Jump	Admin ports	Remote admin
8	Jump → Infra/App/DB	Mgmt ports	PAM-controlled admin
9	Users/Servers → DNS/AD/NTP	53/88/389/636/123	Core services
10	Devices → SIEM	6514/TLS	Central logging

Routers and Layer 3 switches provide comprehensive support for modern networking capabilities, including:

- **Virtual Routing and Forwarding (VRF):** Enables network segmentation and multi-tenant architecture.
- **SNMP (Simple Network Management Protocol):** Allows centralized monitoring and management of devices.

- **NetFlow/IPFIX:** Facilitates detailed traffic analysis and flow-based monitoring.
- **IEEE 802.1X:** Ensures secure network access control through authentication mechanisms.
- **Advanced features:** Support for high-availability, QoS, ACLs, and other next-generation network protocols for performance, scalability, and security.

ITSM : The proposed Helpdesk/Service Desk solution will be fully integrated with the NIC email system to ensure seamless communication and ticket management. End users will be able to raise and track tickets directly through their NIC email accounts, with role-based access controls in place to define their specific privileges (e.g., ticket creation, status tracking, approvals, or escalations). This integration will streamline the support process, enhance accountability, and provide a centralized mechanism for monitoring and resolving user issues efficiently.

K. CYBER SECURITY ASSESSMENT/VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT):

Comprehensive Cyber Security Assessment and VAPT services are required to proactively identify, assess, and mitigate vulnerabilities across NCRB's IT infrastructure, applications, and network. The scope of VAPT shall cover entire NCRB's IT infrastructure, applications, and network including servers, network devices, and virtual machines proposed and migrated by the bidder under this project as mutually agreed upon.

Key features should include the following (but not limited to):

- **Annual VAPT engagements** covering servers, endpoints, web applications, and network devices.
- **Threat modelling and risk profiling** aligned with CERT-In guidelines.
- **Black-box and white-box testing methodologies** to simulate real-world attack scenarios.
- **Detailed remediation reports** with actionable insights and prioritization of vulnerabilities.
- **Post-remediation verification** to validate closure and ensure compliance.

This service will significantly strengthen NCRB's cyber defence posture by ensuring **early threat detection, continuous risk reduction, and compliance readiness**.

L. DEPLOYMENT OF MAN POWER RESOURCES

To ensure seamless operation of the proposed SOC and NOC infrastructure at NCRB, qualified and experienced cybersecurity professionals must be deployed. Their responsibilities will include, but not be limited to, monitoring, incident detection and response, threat analysis, vulnerability and patch management, and overall security operations management as specified below.

SR NO	ROLE	QTY	PREMISES	QUALIFICATIONS AND EXPERIENCE	KEY RESPONSIBILITIES
1.	L1 Analyst (24*7*365)	As per Point No. M	On Site	• Bachelor's Degree in Engineering (B.E./B.Tech) or MCA or equivalent. • Minimum 2 years of experience in SOC/NOC operations. • Certified in CEH / CompTIA Security+ / EC-Council CSA or equivalent.	• Monitor security alerts from SIEM, EDR, and firewall consoles. • Perform initial triage and escalate incidents to L2 if needed. • Maintain security logs, dashboards, and incident reports. • Conduct routine health checks and update threat feeds.
2.	L2 Analyst (5 days in a week)	As per Point No. M	On Site	• Bachelor's Degree in Engineering (B.E./B.Tech) or MCA. • Minimum 4+ years of experience in managing security incidents. • Certified in CISSP / CHFI / CompTIA CySA+ / CEH (Advanced) or equivalent.	• Analyze and validate escalated alerts from L1. • Coordinate incident response, containment, and mitigation. • Tune SIEM rules, configure security policies, and manage threat intelligence feeds. • Support VAPT remediation and compliance tracking.
3.	L3 Analyst	As per Point No. M	Remotely	• B.E./B. Tech/MCA with 6+ years of experience in enterprise cyber security. • Advanced certifications like CISSP, OSCP, or equivalent. • Experience in managing complex incidents, malware analysis, and threat hunting.	• Lead major incident investigations and root cause analysis. • Design and optimize security architecture and response workflows. • Mentor and guide L1 and L2 analysts. • Coordinate with NCRB leadership for strategic advisory and compliance planning.

M. UNPRICED BILL OF MATERIAL-CYBER SECURITY SOLUTION

S. NO	NAME	TOTAL QTY	UOM	FORM FACTOR
	Cyber Security Solutions – Hardware/Software			
1.	Router 10 GBPS (HA Pair)	2	No.	Hardware
2.	HA Pair Firewall, 15 Gbps	4	No.	Hardware
3.	HA Pair 48-Port L3 Core Switches with Latest Features Full Loaded Switch with SFP	2	No.	Hardware
4.	HA Pair 48-Port L3 Distribution Switches with Latest Features Full Loaded Switch with SFP	2	No.	Hardware
5.	Access Layer Switch 48 Ports (L2 Cluster) Full Loaded Switch with SFP for Servers and users switch	19	No.	Hardware
6.	OOB/Management Switch 48 Ports	1	No.	Hardware
7.	Silver-Grade 2-Socket Server, 32 Cores, 512 GB RAM	10	No.	Hardware
8.	Silver-Grade 2-Socket Server, 16 Cores, 128 GB RAM	2	No.	Hardware
9.	400 TB NAS Appliance (10 TB Hot / 390 TB Cold), RAID 6	1	No.	Hardware
10.	500 TB Object Storage for Backup (50 TB Hot / 450 TB Cold)	1	No.	Hardware
11.	SIEM 10000 EPS	1	No.	Software
12.	SOAR	1	No.	Software
13.	Endpoint DLP	500	No.	Software
14.	rsyslog Server (Opensource)	1	No.	Software
15.	NAC Appliance with AAA (HA)	2	No.	Hardware
16.	Patch Management Server 500 Endpoints and 100 VM (RHEL, Windows and Mac)	1	No.	Software
17.	PAM & PIM((Privileged Access Management) and Privileged Identity Management) (for 100 VM)	1	No	Software
18.	Cyber Threat Intelligence (CTI)	1	No	Software(SAAS)
19.	Network Management System (NMS)	1	No.	Software
20.	Windows 2022/2025 STD 16 Core	40	No.	Software
21.	RHEL 9.5 1-2 Socket Lic Virtual	1	No.	Software
22.	Rack 42U (1 Server, 1 Network eqpt., 1 storage)	3	No.	Hardware
23.	12U Rack	6	Nos.	Hardware
24.	High-end PC (i7/32 GB/1TB NVMEs)	6	No.	Hardware
25.	AIO Desktop (i7, 13 Gen or Higher)	350	No.	Hardware
26.	Patch Cord 2 Meter	400	No.	Hardware
27.	Patch Pannel 24 Ports	22	No.	Hardware
28.	Bundle Cat 6 A Shielded	3	No.	Hardware (The quantity is

				indicative and may be vary as per requirement)
	24/7 SOC/NOC Services (On-premises model)			
29.	L1 resources – SOC (24x7x365)	04	No.	
30.	L2 Resources SOC(8x5)	01	No.	
31.	L1 Resources NOC (24x7x365)	04	No.	
32.	L2 Resources NOC (8x5)	01	No.	
33.	L3 Resources -NOC & SOC (24x7 Remote Support)	02	No.	
34.	Training – 2 weeks for overall solutions	1	Set	The duration of training is indicative and may be increased as per requirement
	Security Audit Services			
35.	Cyber Security Assessment/VAPT for a year (IT Infra of NCRB)	3	Yearly	

Note:

- Please Note That All the Hardware's and Software's Should Be Strictly "NTRO Approved Specifications" Only.
- If solution is in the form of software, then the server hardware will also be supplied along with the solution.
- Storage hardware will be supplied for SIEM/SOAR for storing the logs for 365 days.
- Qty mentioned in table is indicative, if offered solution has some of the offered products as integrated part of other products, the same may not be quoted separately, viz. WAF may be integrated with NGFW.
- The detailed specifications of these devices are given in Annexure 'A'.
- All the network devices need to be hardened as per the minimum baseline device hardening measures specified in Annexure 'B'. These listed measures are indicative and not exhaustive. Final measures adopted for hardening of all devices will be decided based on consent of NCRB management.
- The entire SOC/NOC setup should have the minimum baseline capabilities specified in Annexure 'C'. The listed requirements are indicative and not exhaustive. Final requirements will be decided based on consent of NCRB management. The detailed specifications & other requirements of the devices to be deployed in NOC/SOC setup are already given in Annexure 'A'.
- All ICT equipment must be manufactured within one year prior to the project implementation date.
- As NCRB is already in possession of an active license for the Antivirus and Backup solution, the same has not been included in the present Bill of Quantities (BOQ) proposal.
- Automatic ingestion of threat intelligence feeds into SIEM and Next-Generation Firewalls (NGFW) from NCIIPC, NTRO, and the Threat Dissemination Platform (TDP).
- Servers, storage systems, desktops, and workstations must be supplied by the same OEM.
- The OEM must maintain authorized service centers in all major metropolitan cities of India.
- Each OEM shall ensure the provision of the highest level of technical support.
- The manpower duration for SOC and NOC shall be specified for a period of three years. The personnel will be deployed across shifts as per point L & M.
- Networking and OS hardening activities, along with package installation for application deployment, will be carried by the vendor.

- The scope of audit is specified in point K. The vendor will also assist in patching audit issues related to the network and infrastructure, excluding application development and database optimizations.
- For the SOC & NOC, vendor will provide 24×7 on-site L1 coverage at the NCRB office, L2 coverage during business hours, and 24×7 remote L3 support.
- The edge NGFW and the internal NGFW will be sourced from different OEM's, thereby enhancing supply-chain resilience and technology diversity.
- Dedicated NTP Server setup along with backup setup will be done/provided by vendor.
- The vendor will configure a RHEL-based rsyslog server to collect logs from CCTNS and other critical applications and forward them to the primary SIEM.

Hardware WARRANTY AND Software Support

- 5 Years OEM warranty from the date of installation of all cyber security hardware & Software to be installed at NCRB HQ . All hardware support will be provided onsite.
- Software support for 5 years will be provided by vendor post Go-Live.
- The complete support of the configured solution will be provided by vendor for next 5 years which includes VM, server, storage, network etc. excluding application development and DB optimization support. The vendor will also assist in patching audit issues related to the network and infrastructure, excluding application development and database optimizations.

N. DELIVERY TIMELINES (TENTATIVE)

Below are the tentative time lines for the delivery of cyber security solutions to NCRB HQ.

ACTIVITIES	TIME	MILESTONE
Project Kick off	T1	Milestone-1
Delivery/Supply of equipment/licenses/hardware's	T1+ 20 weeks= T2	
Hardware and Software Installation, Configuration, Networking, Creation of VMs and Migration	T2+ 12 weeks= T3	Milestone-2
Testing and validation	T3+ 2 weeks= T4	Milestone-3
Go Live	T4+2 Weeks = T5	
Operational Training	T5+2 weeks = T6	

Total Time for implementation will be Approx. 38 weeks.

ACTIVITIES	SUB-ACTIONS (High Level)	MILESTONE / OUTPUT
Project Kick-off	• Finalize scope, objectives, success criteria • Governance & RACI; escalation paths • Site-readiness checklist (power, cooling, racks, access) • Risk register & mitigation • Access pre-requisites (VPN,	**Milestone-1:** Kick-off complete; plan signed-off

	accounts) • Master plan & schedule baseline	
Delivery / Supply (HW, licenses)	• Freeze BoM; raise POs • Vendor coordination & shipment tracking • Site readiness (rack space, PDUs, cable trays) • Receive & QA hardware; inventory & tag • Activate licenses / subscriptions	**Milestone-1:** Materials on-site; licenses active
Installation, Configuration & VM Creation (Data Center Build)	**Racking & Stacking:** mount, power, cabling **Routing & Switching:** VLANs/trunks, LACP, MTU, QoS, IP plan **Enterprise Network Hardening:** AAA/RBAC, SSH, SNMPv3, syslog/NTP, ACLs, baseline NGFW/WAF policies **Hypervisor Setup:** cluster, storage/datastores, vSwitch/vDS/port-groups, HA/DRS, time sync **VM Provisioning and Migration:** templates/golden image, sizing, IPs/LVM/filesystems **OS Hardening:** baseline CIS/NIST controls, patching **Packages/Prereqs:** app runtimes, agents, tools	**Milestone-2:** DC built & baseline complete
Testing & Validation	• Infra validation (network, hypervisor, VM health) • Security checks (ports, policies, hardening spot-checks) • NCRB application testing (functional/UAT) • Performance & failover smoke tests • Defect fixing & re-test; UAT sign-off	**Milestone-3:** UAT / validation sign-off
Go-Live	• Final data sync & cutover runbook • Approved change window • DNS/NAT/Firewall updates; traffic switch • Health monitoring & rollback guardrails • DR replication posture verified	**Milestone-3:** Production cutover complete
Operational Training & Handover	• Admin/operator training (Day-0/1/2 playbooks) • Runbooks & SOPs (backup, restore, monitoring) • Support contacts & warranty artefacts	**Milestone-3:** Handover & project closure

	• Final documentation & acceptance	

O. PAYMENT TERMS

Payment for the services rendered shall be released as per the following milestones:

SL. NO.	DELIVERABLES	TIMELINE	PAYMENT
1.	Delivery of all items at NCRB (as per Point M)	Milestone-1	25% of CAPEX value
2.	Installation and Commissioning of all Hardware items (as per Point M) at NCRB including Networking	Milestone-2(a)	25 % of CAPEX value
3.	Installation and Commissioning of all Software items (as per Point M) at NCRB including Creation of VMs and Migration	Milestone-2(b)	25 % of CAPEX value
4.	Testing, validation, Go-live & Operational Training	Milestone-3 + 3 months (3 months after successful completion of Milestone-3)	25% of CAPEX value
SL. NO.	**DELIVERABLES**	**TIMELINE**	**PAYMENT**
1.	Deployment of manpower for O&M of SOC and NOC	Post Go-live	Quarterly, based on quoted OPEX cost
2.	Software Support	Post Go-live	Quarterly, based on quoted OPEX cost
3.	Cyber Security Assessment/VAPT for IT Infra of NCRB	Post Go-live	Yearly, based on quoted OPEX cost

- The manpower duration for SOC and NOC monitoring post go live shall be specified for a period of three years. The personnel will be deployed across shifts as per point L & M.
- Software support for 5 years will be provided by vendor post Go-Live. The complete support of the configured solution will be provided by vendor for next 5 years which includes VM, server, storage, network etc. excluding application development and DB optimization support.
- The scope of audit is specified in point K. The vendor will also assist in patching audit issues related to the network and infrastructure, excluding application development and database optimizations.

Note-:
All that is required to make it Fully Functioned shall be supported at No Extra Cost. Any cable, part, accessories, items (electronic or otherwise) which are not listed but are required to make the products successful and functional in entirety, will be supplied by the bidder at no extra cost.

CAPEX refers to the **one-time cost** incurred for the procurement, delivery, installation, and commissioning of cyber security hardware, software licenses, infrastructure components, and related systems. It includes all fixed assets required to operationalize the SOC and NOC environments at NCRB.

OPEX covers the **recurring expenses** associated with post-deployment activities, including manpower deployment, system upkeep, technical support, monitoring services, and routine software updates as part of the ongoing operations and maintenance phase.

P. LIQUIDATED DAMAGES

In the event of a delay in delivery or implementation attributable solely to the vendor, **liquidated damages may be levied at a maximum of 0.1% of the delayed deliverable's value per week**, subject to a ceiling of **10% of the total contract value**.

However, delays caused due to **force majeure events, dependencies on third-party clearances from NCRB side, site readiness issues, or delays not attributable to the vendor** shall be duly excluded from the LD clause upon mutual agreement.

This ensures a **balanced and just framework**, protecting the interests of both NCRB and the vendor while promoting timely and effective execution of the project.

Q. SERVICE LEVEL AGREEMENT (SLA)

The vendor shall maintain the following minimum service levels during the operations and maintenance phase of the project. These SLAs are designed to ensure optimal system performance while allowing flexibility for real-world operational conditions:

Parameter	Minimum Uptime / Availability
Cyber Security Infrastructure Availability	≥ 98.0% annually
SOC / NOC Application Availability	≥ 98.0% annually
Manpower Availability (L1 Analysts)	≥ 98.0% annually
Manpower Availability (L2 Analysts)	≥ 98.0% annually
Manpower Availability (L3 Analysts)	≥ 98.0% annually
Response Time for Critical Alerts	≤ 30 minutes
Resolution Time (based on severity)	As per mutually agreed matrix

Note-:
RTO(Recovery Time Objective) will be 8 Hours (down time)
RPO((Recovery Point Objective)) will be 3 Hours (data loss)

- SLAs will be evaluated **quarterly** with a 15-day reconciliation window.
- **Exceptions such as planned maintenance, force majeure, dependencies on third-party clearances from NCRB side, or delays not attributable to the vendor** will be excluded from SLA calculations.
- Any applicable penalties or credits will be subject to mutual discussion and resolution at the time of performance review.

R. SUB-CONTRACTING

The vendor shall remain the **principal contractor and single point of accountability** for the successful execution of the project. However, to ensure timely and efficient delivery, vendor reserves the right to **sub-contract specific non-core activities** such as:

- Site preparation (civil/electrical works)
- Structured cabling and hardware installation
- Facility management and logistics support
- OEM-authorized product integration and support services

All subcontracted activities will be performed under **strict supervision and quality assurance** by vendor, ensuring full compliance with the scope, standards, and security policies defined by NCRB. Under no circumstances shall core responsibilities such as **cybersecurity design, policy enforcement, and SOC/NOC operations** be outsourced. The vendor shall remain **fully responsible and liable** for all deliverables, timelines, and SLAs committed.

S. UNDERSTANDING & CONDITIONS

To ensure smooth execution and clarity of responsibilities, the following understanding and conditions are considered applicable for the project:

- **Site Readiness**: NCRB will ensure availability of required physical infrastructure (racks, power, earthing, AC, and space) prior to equipment installation.
- **Connectivity Provisioning**: Internet bandwidth, MPLS/VPN lines, and required ISP coordination for threat intelligence updates will be provided by NCRB.
- **Access & Permissions**: Timely access to NCRB premises, IT infrastructure, and designated officials will be ensured for smooth execution and support.
- **Exclusion of Force Majeure**: Delays or non-performance due to natural disasters, events beyond vendor control shall be exempt from penalties.
- **Data Access Responsibility**: NCRB shall remain the data owner and shall govern all data classification, access rights, and retention policies.
- NCRB will be responsible for provisioning required internet bandwidth, leased lines, and other connectivity (e.g., for threat intelligence updates and remote support).
- The SIEM solution will be sized for **10,000 EPS sustained capacity**, with support for a **11,000 EPS peak load**. Any scaling beyond this will be addressed separately.
- NCRB will ensure availability of essential infrastructure at deployment locations, including:
    - Adequate rack space
    - UPS-backed power
    - Air conditioning
    - Proper earthing and physical security
- Technical training for NCRB teams will be conducted by vendor, jointly with OEMs or certified training partners, covering product usage, monitoring, and response.
- High-end PCs will be procured from reputed OEMs such as **Dell, HP, Lenovo, or** as per the acceptance by NCRB.
- Any change in scope, user volume, or feature set after contract award will follow a formal **Change Request (CR) process**, including commercial and timeline alignment.
- The vendor will not be liable for disruptions caused by:
    - Site inaccessibility
    - Delays in power/network availability
    - External events such as ISP outages or infrastructure faults beyond vendor control
- NCRB will be responsible for internal data access policies, classification, and user roles in alignment with **CERT-In**, **NIC** guidelines.
- NCRB and vendor will collaborate proactively to address project risks, expedite decisions, and facilitate support from OEMs and other third-parties as needed.
- All core cybersecurity components including **NGFW, SIEM, SOAR, and NAC** will be sourced from **internationally reputed OEMs** that are recognized for their proven security technologies.
- The vendor shall act as a **System Integrator (SI) and Solution Provider**, and does not claim to be the **original equipment manufacturer (OEM) or intellectual property owner** of any of the proposed third-party cybersecurity products.
- The **features, functions, and capabilities** described in the proposal documents are based on current product specifications available in public and OEM documentation at the time of submission.
- Any **OEM-driven changes, feature deprecation, or enhancement limitations** encountered during implementation will be addressed through alternate configuration or workaround options within the contractual scope, where feasible.

- Final product selection will comply with technical requirements of NCRB and government cyber guidelines, and may be subject to **equivalent substitutions** in line with OEM supportability and product lifecycle status.
- Integration and interoperability between multi-vendor components will be designed **as per available APIs, OEM documentation, and configuration support**.
- Any custom integration, where **standard interoperability is not natively supported**, will be assessed through a change request (CR) and may involve additional timelines or resources, if required.
- All product configurations will adhere to **best practices recommended by OEMs**, with security hardening applied in accordance with CERT-In and ISO 27001 guidelines.
- Product warranties will be honoured **as per OEM terms**, and vendor will coordinate with respective OEMs for license activation, defect resolution, and firmware/software upgrades.
- In the event of **end-of-life (EOL) declaration** by an OEM during the project period, equivalent alternate models or upgrades will be proposed for NCRB's review and approval.
- The vendor will be responsible for the **design, deployment, training, and overall integration** of the cyber security architecture.
- NCRB shall approve the final OEM selections during the project's detailed design phase, subject to functional compliance and certification requirements (e.g., STQC, Common Criteria, etc.).
- The vendor will be responsible for the execution of the project and will bear all the cost related to the Hardware, Software, Licenses etc. needed for the execution and implementation of the project successfully.
- NCRB will have no additional liability to pay after entering the project. Any cable, part, accessories, items (electronic or otherwise) which are not listed but are required to make the products successful and functional in entirety, will be supplied by the bidder at no extra cost.
- Compliance to NCRF (National Cyber Reference Framework) Guidelines to be ensured by the bidder/vendor/contractor.
- All equipment manufacturing dates should not be more than 01 year from the project purchase date.
- VAPT/Audit to be done annually by CERT-In empanelled vendor. The cost to be paid by SI/vendor. However, selection of Auditor to be done in consultation with the purchaser. The scope of audit is specified in point K. The vendor will also assist in patching audit issues related to the network and infrastructure, excluding application development and database optimizations.

T. Additional Terms & Conditions

1. **Bid is invited from Public Sector Enterprises (PSEs) only.**
2. Bidder must quote CAPEX and OPEX price separately. However, L1 will be decided on the basis of Total value-wise evaluation (Total Project Cost) i.e. CAPEX + OPEX. **The quoted CAPEX amount/price should not be more than 70% of the Total Project Cost (CAPEX + OPEX).**
3. e-PBG percentage will be **3%** with validity of atleast **62 months post Go-live.**
4. **Evaluation of Bids**- Considering the technical complexity and criticality of the project, the evaluation of the bids will be based on **Quality-cum-Cost Based Selection ("QCBS") method as per GFR rules.**

   (a) Technical bids will be evaluated for various parameters as specified hereinafter and the technical score secured by bidders in technical evaluation will be considered for further evaluation of bids. Only those responsive proposals that have achieved at least **minimum specified qualifying technical score (50%)** in quality of technical proposal will be considered

further for the next stage. Each criterion mentioned under QCBS shall be marked as per the documentary evidence provided by the bidder.

S.No.	Criteria Category	Evaluation Criterion	Max Marks	Supporting Documents Required
A	**Bidder's profile**		**35**	
A1	Average Annual Turnover Average annual turnover over the last three financial years(FY 2022-2023, FY 2023-2024, FY 2024-2025)	(a) More than 200 Crores (10 marks) (b) More than 150 Crores but Less than/Equal to 200 Crores (8 marks) (c) More than 125 Crores but Less than/Equal to 150 Crores (6 marks) (d) Less than/Equal to 125 Crores (4 marks)	10	Certificate from the Statutory Auditor/Company Secretary on turnover details from the over the last three (3) financial years.
A2	**Manpower** Full time employees on payroll of bidder working in the business unit providing "IT/ITeS" services as on bid submission date	(a) More than 100 (10 marks) (b) More than 50 but Less than/Equal to 100 (8 marks) (c) More than 25 but Less than/Equal to 50 (6 marks) (d) Less than /Equal to 25 (4 marks)	10	Certificate from the Head of HR Department or equivalent on bidding entity's letter head countersigned by authorized signatory.
A3	**Certifications**	ISO 9001 (2 Marks) ISO 27001 (2 Marks) ISO 14001(2 Marks) ISO 20000 (2 Marks) ISO 45001 (2 Marks) CMMi Level 3 or higher (5 Marks)	15	Valid Certificates
B	**Project Experience**		**25**	

B1	The Bidder should have completed projects in IT/ITeS including manpower with minimum value of INR 30 CR and above during last three (3) years as on bid submission date.	(a) More than/Equal to 10 projects (25 marks) (b) Between 6-9 projects (15 marks) (c) Between 3-5 projects (10 marks) (d) Less than 3 projects (5 marks)	25	Work Order + Certificates of Completion (Certified by the Statutory Auditor/Company Secretary).
C	**Technical Presentation**		**40**	
C1	Presentation for understanding of Current requirement as per scope of work, proposed service approach, methodology, work plan for performing the assignment etc.	Technical presentation should cover: • Details of proposed deployment plan, manpower retention strategies and handling of staff resignation including provision of a backup pool. • Detailed approach & methodology for providing technical support to the project, capacity building for resources and Escalation Matrix. • Proper readable Document submission as well as proper indexing	40	Bidder should have to submit detailed Approach and Methodology with Bid document.

(b) After opening and scoring the Financial proposals of responsive technically qualified bidders, a final combined score is arrived at by giving predefined relative weightages for the score of quality of the technical proposal and the score of financial proposal. The scores of the Technical and Financial Bids will be assigned weights as under: **Technical Score: 70%; Financial Score: 30%.** The proposal with the highest weighted combined score (quality and cost) shall be selected.

(c) NCRB reserves the right to modify / amend the evaluation process at any time during the Bid process, without assigning any reason. Any time during the process of evaluation, NCRB may seek specific clarifications from any or all the Bidders. NCRB's decision in this regard shall be final & binding.

ANNEXURE 'A'

A. DETAILED SPECIFICATIONS

1. Detailed Specification of Router 10 GBPS (HA Pair)

Sl. No	Router	Compliance	Cross Reference
1.	Device should have minimum 4x 1/10G SFP interfaces populated with 2*10G SR SFP, 2*10G LR SFP & 4*1/10G RJ45 ports		
2.	Device should have additional interface modules/slot support for future expansion of onboard interfaces		
3.	Device should support port ACL with L3 and L4 parameters		
4.	Device support LLDP and LACP to bundle links and detect mis cabling issues.		
5.	Device should support Routing Protocols: OSPFv2, BGP, IS-IS, and RIPv2		
6.	Device Should support BFD		
7.	Device Should support VRRP V4		
8.	Device should support VXLAN+EVPN overlay technology		
9.	Device should support NAT		
10.	Device should support VRF		
11.	Device should be able to support 1M or higher IPv4 routes		
12.	Device should be able to support minimum 128 IPSEC tunnels with AES256 encryption		
13.	Device should support minimum 5 Gbps encrypted throughput and an aggregate throughput of 30 Gbps		
14.	Device should be able to support GRE tunnels		
15.	Hardware should be able to work as traditional router and capable of upgrading to SDWAN router with additional license, if required in future		
16.	Device should support software hitless patching		
17.	Device should support maintenance mode/ Graceful insertion and removal (GIR) to isolate device from the network in order to perform debugging or an upgrade while gracefully steering traffic to peer nodes		
18.	Device should 1+1 redundant Fans		
19.	Device should support 1+1 redundant & hot-swappable power with support for AC power supply options.		
20.	Should be able to provide application awareness of application by performing DPI and subsequently, load-balance the application across multiple available paths based on various factors (like BW, delay, latency etc)		
21.	Should support Control Plane protection (CoPP)		
22.	Should support port ACL with L3 and L4 parameters		

23.	Should support port-based DOS protection (PDP)		
24.	Should have programmability and automation support with on board bash, python, C++, GO & Open Configuration.		
25.	Should support in-band telemetry		
26.	Should support 8 queues per port		
27.	Should support priority queue		
28.	Should support ACL based classification for QoS		
29.	Should support rate limiting function like policing and shaping		
30.	Device to be provided with licencing and application to provide centralised and unified monitoring, provisioning & telemetry solution and integration dashboard supporting detailed topology view, time-series based database visibility, anomaly/deviation analysis, bug/PSIRT visibility, device resource utilization, traffic flow analytics, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts, Change workflow management, congestion monitoring, tracking changes in MAC table, Multicast Table, ARP, IPv6 neighbour table and IPv4, v6 route table for troubleshooting purpose, notification through email & msg, 3rd party integration. SI will factor required VM's to install the software or on MEITY approved Cloud, if any OEM wants to supply their Appliance they allowed to in HA Cluster		
31.	Hardware and TAC support should be quoted directly from the OEM. OEM should have 24x7 TAC support.		
32.	Should be NDcPP/EAL common criteria certified.		
33.	Operating temperature of 0°C to 40°C		
34.	Manufacturer Authorization is Required		
35.	All licences should be provided with the devices for the mentioned features from Day 1. All Ports should be activated from Day 1. All asked feature lic should be supplied from Day 1. Hardware & Software Support as per Hardware WARRANTY AND Software Support clause defined in point M of this document		
36.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted as per Hardware WARRANTY AND Software Support clause defined in point M of this document along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. Quoted product should have 8 years life Cycle from date of delivery at Site and same need to be mentioned in Signed MAF.		
37.	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.		
38.	Manufacturer Authorization is Required		

39.	Quoted product should be latest and should be support for minimum 8 years from the date of delivery at Site and same need to mentioned in signed MAF		
40.	Bidder should submit fully complied solution; any deviation will result in bid rejection and Intentional wrong compliance claims will result in blacklisting of OEM & Bidder for next 3 years		
41.	Specification mentioned is minimum requirement and any Bidder / OEM can quote higher configuration if required.		
42.	Manufacturer Authorization is Required. Specification mentioned are minimum and any OEM/SI can quote higher specifications.		

2. Detailed Specifications for Firewall (NGF)

a. Edge Firewall 15 GBPS

S/N	General Hardware Specification	Compliance (Yes/No)
1.	The Firewall appliance must be non-ASIC based and should have Multi core architecture to mitigate against the sophisticated threats. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet (without ASIC)	
2.	The Firewall appliance must have a hardened operating system from the OEM and should have 8 Core CPU with 64 GB of RAM to make sure all the security capabilities are provided without degradation form day one.	
3.	**The Firewall appliance must have minimum 8x10G and 8x1G Ports from day 1 with required SR transceivers as per the ports. Also, should have additional network I/O slot to add 4x100G or 8x40G or 25G ports in future, depending upon organisation's choice.**	
4.	The Firewall appliance should not be more than 2U rack-mounted design and must have redundant hot swappable power supply to remove any single point of failure.	
5.	The Firewall appliance must deliver 15 Gbps NGFW throughput with Security features (FW, IPS, and Application Control) enabled and 10 Gbps Threat Prevention throughput. The same must be available in the public datasheet.	
6.	The Firewall appliance must deliver 50 Gbps of IPSEC VPN throughput from day 1 without any limitation of VPN Clients.	
7.	The Firewall appliance must deliver 650K new connections/sessions per sec and 50 million concurrent connections/sessions from day1.	

8.	The Firewall appliance must have the security features including IPS, Application Awareness, Anti-Bot, DOS prevention, URL filtering, Anti-Malware, AETs including routing features to be managed from the Central console, no need for any configuration via appliance GUI and Appliance CLI. Solution also support integration with Snort.	
9.	The Firewall appliance must support L3 protocol functionality like Static & policy-based routing, static multicast routing, dynamic routing like MP-BGP, RIPng, OSPF(v2 & v3), IGMP proxy, BGP, BFD, PIM (SM & SSM), and Application-aware routing	
10.	The Firewall appliance must support IPv4 and IPv6 from day 1 with NAT66, NAT64, NAT46 and PAT from day 1	
11.	The Firewall appliance must support IPv6 capability including Dual stack IPv4/IPv6, ICMPv6, DNSv6, IPv6 static, SLAAC, DHCPv6 relay	
12.	The Firewall appliance must support TLS 1.3 and TLS/SSL server certificate verification before decryption decision is taken	
13.	The Firewall appliance must support security proxies for the following TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS	
14.	The Firewall appliance must have Firewall for stateful blocking, URL filtering, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections	
15.	The solution must support client-based agent to check the security posture of endpoints and must be able to employ policies basis the attributes. Policy must be defined on NGFW for discarding the user requests if AV is not updated, OS version is Obsolete, Load on Endpoint is high / any users is using the obsolete browsers and should not have any dependencies on the number of clients supported & there should not be any license attached to it.	
16.	The solution must support high availability and load balancing between multiple ISPs, including VPN connections, Multi-Link VPN link aggregation, QoS-based link selection and admin should be able to manipulate the sensitivity of an application based on jitter, packet loss & latency	
17.	The solution must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active software or configuration.	
18.	The Firewall appliance inspection engine must deliver more than 10000 fingerprint/vulnerabilities for detecting exploit attempts against known vulnerabilities in protocol specific tcp/udp port number. Solution must provide multi-layer inspection to increase network security and performance and it should combine access control to define policies that govern your user's access to network resources, deep inspection to detect advanced threats & file filtering to block malicious file transfers.	

19.	The solution must support 7000+ Applications for better control and visibility throughout the environment so that solution should be able to understand applications like 4sync,4tube, bizible, Facebook, YouTube etc. and should support QUIC & HTTP/3	
20.	The Firewall appliance Inspection Engine/ Anti-Bot must employ the below inspection technologies 1. Multilayer traffic normalization 2. Vulnerability-based fingerprints 3. Evasion and anomaly logging 4. Decryption-based detection 5. Message length sequence analysis	
21.	The solution must support FTP and DNS Proxy to restrict the types of traffic and the commands that can be used with DNS and FTP connections. Solution must support DNS sink holing for UDP and TCP service.	
22.	The solution must provide steering of applications dynamically & should provide application identification with link monitoring to effectively allocate networking resources, ensuring that the critical applications receive the necessary resources for optimal performance.	
23.	The solution must have the technique for monitoring the application health and provide visibility into the organization's network traffic and the administrators should be able detect and resolve bottlenecks before they become a network-wide problem & should provide real-time visibility, historical views, and easy access to connectivity logs directly from the OEM Centralized management dashboard.	
24.	The solution should have an option to create alternative policies if the connectivity between the NGFW and central Manager is lost; any policy should be allowed to be selected whether it is a normal policy or one of the alternative policies	
25.	The solution must prevent against the websites via URL filtering that mask their identity using Dynamic DNS services, Elevated exposure by website that camouflage their true nature, domain name that are registered recently, parked domain, Unauthorized Mobile Marketplaces to prevent users visiting the websites that may distribute applications unauthorized by the mobile OS manufacture	
26.	Solution must be able to prevent the users to visit the websites that use technologies that alter the operation of a user's hardware, software, or network to decrease owner's control with the intent to gain fraudulent access and with potential malicious intent.	
27.	Solution must be able to prevent the users to visit the websites that enable download of software applications or file download servers, download of media content, client software to enable peer-to-peer file sharing and transfer, Sites that store personal files on web servers for backup or exchange.	

28.	Solution should support Re-authentication when using browser-based user authentication and support 4096-bit RSA key for Browser Based User Authentication.	
29.	The solution must have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and blocks access to known malicious sites and non-existent IP addresses with ability to proactively measure against command and control (C2) access & second-stage malware downloads for disrupting the communication between infected endpoints and attackers	
30.	The solution must provide visibility into application health history along with health status history of network applications.	
31.	Solution should have more than 95 URL categories and should support more than 50 languages for better and effective web controls.	
32.	Solution must support File Filtering via Policy for minimum 200 file types in 15 categories and also support file Reputation checking & blocking for file with Malware reputation	
33.	The solution must support custom script upload via Centralize manager so that same script can be used on multiple NGFW and it should support using FQDN to connect between the Firewall and management server & Log Server.	
34.	The solution must support minimum 2000 devices management capability along with SDWAN function and Multi-Layer Traffic Normalization/Full-Stream Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic (both TLS 1.2 and 1.3), Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti-Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods, Automatic Updates	
35.	The management platform must be a dedicated OEM appliance/software/VM running on server and should be capable of managing all the firewalls from day 1 and should be scalable for upto 100 firewalls.	
36.	The solution should come with a web-based administration interface in the dedicated centralized manager and must be able to define the custom roles in addition to predefined roles (e.g., Owner, Viewer, Operator, Editor, Super User) to control permissions flexibly and accurately.	
37.	The centralized management platform must be sized for handling all the managed firewall logs but should not have any licensing limitation on logs per day. Management and log server should have minimum 16 cores, 32 GB RAM with 2 TB log storage capacity.	

38.	Solution should support local user creation options via Central Manager and also support the use of external CA issued certificates in internal management communication and Centralized manager should support to block the access temporarily after multiple failed logon attempts from the same IP.	
39.	The solution must have the ability to support high availability of different model /appliances and versions within the same HA cluster	
40.	The OEM should have presence in India for last 15 years or more and must have Support Center and Registered Office in India to provide sales and support.	
41.	Firewall supports traffic blocking based on custom IP ranges, individual IPs, IP lists, and domain lists. It can integrate with third-party (NTRO, Cert-IN etc) threat intelligence feeds and apply custom URL category filtering.	
42.	VRF supported	

NGFW Software & Maintenance Support

Item	Description of Requirement
Software and Support Maintenance	The OEM should have 24x7, 365-day TAC support.
	SSLVPN Solution should be a dedicated Remote Access VPN solution running on a virtual appliance allowing users to securely access corporate applications and network when they are connecting from an untrusted network.
	SSLVPN Remote Access solution must be deployed as a dedicated solution and it should not be running on a Firewall, UTM, Load Balancer, etc.
	The solution should be a Next Generation SSLVPN supporting Clientless Web Portal based VPN access out-of-the-box without any dependency on additional component or solution.
	The solution should support Agent based Layer 3 VPN capability out-of-the-box without any dependency on additional component or solution.
	The solution should support Agent based Layer 4 VPN capability out-of-the-box without any dependency on additional component or solution. Solution should allow VPN admin to create policies or rules based on Application instead of IP address or service.
	The solution should have a unified Agent that can work with different technologies like Remote Access VPN, nZTA and NAC solution to reduce agent overhead.
	The solution should support Active-Sync Proxy capability out-of-the-box without any dependency on additional component or solution allowing users to securely access emails on their Smart Phones.
	The solution should support Single Sign-On capability for local, public and SaaS based applications. SSO should be available out-of-the-box without any dependency on additional component or solution.

	The solution should support Multifactor Authentication for VPN connection with Token based authentication. The proposed solution should have built-in OTP server for 2FA/MFA authentication.
	The solution should not be dependent on another solution like NAC for posture assessment of the VPN user/device. The proposed SSLVPN solution must have a built-in Posturing capabilities for Windows, Macintosh, Linux, Android and iOS devices.
	The solution must support authentication and authorization of VPN user's device before establishing a VPN connection or tunnel. The solution should be able to restrict VPN access from unauthorized BYOD devices.
	The solution should be capable to do the finger printing of devices trying to connect to the setup and capture at least 3 unique identifiers like MAC address, Digital-Certificate, Computers AD account, etc.
	The solution should be able to prevent cross site scripting attacks and should support following web security mechanisms
	HTTP Only
	HTTP Strict Transport Security (HSTS)
	X-Content-Type-Options
	The solution should have persistent cookie options that allows to choose whether to preserve or delete persistent cookies when a session is terminated.
	The solution should support lock out option to protect the system (SSLVPN Gateway) from denial of service (DoS), distributed denial of service (DDoS), and password-guessing attacks.
	The solution should support X-Frame-Options protection to defend against click-jacking attacks by adding X-Frame-Option header to all the SSLVPN generated pages.
	The solution should have support for Slow Post Attack Defense to protect SSLVPN gateway against slow-post DOS attacks from non-authenticated users
	The solution should have Integrity checking option to configure and scan the SSLVPN gateway to periodically check for any integrity anomalies. If any anomaly found, information should be displayed in the dashboard.
	The solution should support configuring custom HTTP Headers to prevent attacks like XSS.
	The solution should support Deletion of all cookies at session termination.
	The provided solution should support TLS 1.3 version.
	The provided solution should support AES256 and SHA2 ciphers.
	The solution should be capable of providing secured remote access to the organizations Corporate Web Portals, Applications and Desktops to the users connecting from external network through a secured VPN connection.
	The solution should be accessible from all variety of devices like desktops, laptops, tablets, mobile phones, etc. having Windows, Linux, Mac, Android, iOS and Chrome OS through all major browsers like Chrome, Edge, Safari, Firefox, etc.
	The solution should support centralized and decentralized deployment.
	The solution should not have dependency on a direct cable connection between cluster devices and should support cluster formation, communication and data/session synchronization over the network.

	The solution should support Remote Access VPN capabilities with agentless and agent based Posturing, SSO and MFA capabilities from day 1. Bidder needs to provide concurrent licenses to support all the listed capabilities for 'X' number of concurrent user connections from day 1.
	Should support scheduling of configuration and log backup to external system
	Configuration should be able to be restored from back up/ archive
Clientless access	SSL VPN solution should support clientless portal-based access to web application and windows file shares.
	Should support URL masking of internal FQDN and IP addresses
	Should maintain original server access control policies while accessing the file resources through VPN
	Must support Single Sign-On (SSO) for web-based applications and web-based file server access
	Must should support RDP/Telnet/SSH sessions using HTML5 for clientless access with SSO support
	Must support restricting copy/Pasting of data from Target RDP/SSH system to the user system and vice versa without agent
	Solution should support access to VDI servers
	Must support Active Sync proxy for secure Email access from Mobile Devices
Agent Access	VPN Agent must have Layer-3 IPsec VPN support with SSL and ESP transport mode. It should allow admin to customize ESP port number for data channel.
	The proposed solution should support ESP to SSL fallback for data channel in Layer 3 VPN mode
	VPN Agent must have Layer-4 Per-App VPN capabilities for client/server applications to provide for maximum data security and user transparency.
	Must have Location Awareness intelligence for triggering the VPN connection automatically based on the advice location.
	Must support advance VPN capabilities like Always-ON VPN with Lock Down capabilities
	Solution must support Exception rules for Lock Down Access
	Solution should support Dual-transport (SSL + Encapsulating Security Payload) full Layer 3 VPN connectivity with granular access control like "VPN Only Access" modes for Compliance.
	Solution should support Full range of split tunnelling options which are configurable, including support for individual IP addresses as well as FQDN. It should include enable and disable functionality with overriding route capability and route monitoring.
	Must support Full Tunnel VPN mode.
	Must support dynamic connection update to enforce the policy changes seamlessly without much admin intervention.
	Must have a flexibility to preserve client-side proxy setting or enforce internal proxy setting to remote user system.
	Must support running session start and session end scripts to map the network drives automatically post VPN connection.
	The solution should support Wireless suppression.

	Must support Credential Provider capabilities to authenticate users by establish the VPN connection before desktop login.
	Must have a capability to integrate with following authentication Servers: - a) Active Directory b) LDAP c) RADIUS d) Local database f) Certificate based authentication g) SAML 2.0 and Oath h) TOTP Solution should have support for following multifactor authentication Methods: a) LDAP or AD based Username Password and Certificate based authentication. b) User Credentials and Soft Token c) Machine fingerprinting based validation with MAC Address and digital certificates above all authentication methods should be implemented from day 1. Must support password management for allowing remote users to reset their passwords and receive notifications about password expiry.
Endpoint Compliance/Posture Check	Solution must support both PRE and POST compliance check capabilities where compliance check can be performed even before the user authentication.
Endpoint Compliance/Posture Check Auto Remediation	Solution must have stateful compliance check capabilities to immediately identity any change in device compliance after VPN connection and take the required action against it.
	Compliance check must be supported with a Persistent and temporal agent
	Must support compliance check on different platforms like Windows, MAC OSX, Linux, IOS, Android, Chrome OS, Windows Phone.
	The proposed solution must have granular compliance check options for Windows devices which includes the following:
	Hard drive encryption detection
	Detection of Pre-defined Antivirus, Personal Firewall and Antispyware
	OS Check, CVE Check (known vulnerability detection)
	Processes, Registry Check
	Files, TCP or UDP Ports Check
	NetBIOS, MAC address Check
	Patch Check by integration with Patch Management Solution
	Machine Certificate check
	Rooted or Jail-broken
	OS Version
	Solution must support auto-remediation capabilities out-of-the-box.
Auto Remediation Regulatory Compliance	Solution must support enabling Antivirus application, starting virus definition file download and starting system scan.
	Solution must support kill processes, delete files option as part of Auto Remediation

Regulatory Compliance Administration, Management, Reporting and Logging	Sharing customized notifications in case of compliance failure
	Solution must support adding/changing system registry through Autor Remediation
	The proposed solution must comply to the following industries recognized certifications:
	NIAP
	FIPS-2 /NIST
	NDcPP
	SSL VPN should provide Role based access control for administration of SSLVPN. It should allow using AD/LDAP based authentication for device administrator with MFA option.
Administration, Management, Reporting and Logging	Solution should Have built-in reporting capabilities to track details like User login/logout, Total time spent on VPN, Average time spend on VPN, Compliance Report, Device report, OS details, etc.
	Should have support Direct Serial Console CLI and Web GUI access on the device
	The solution should support integration with SIEM and SNMP tools for device health monitoring and alerting mechanism.

b. Internal Perimeter Firewall 15 GBPS

S/N	General Hardware Specification	Compliance (Yes/No)
1.	The Firewall appliance must be non-ASIC based and should have Multi core architecture to mitigate against the sophisticated threats. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet (without ASIC)	
2.	The Firewall appliance must have a hardened operating system from the OEM and should have 8 Core CPU with 64 GB of RAM to make sure all the security capabilities are provided without degradation form day one.	
3.	**The Firewall appliance must have minimum 8x10G and 8x1G Ports from day 1 with required SR transceivers as per the ports. Also, should have additional network I/O slot to add 4x100G or 8x40G or 25G ports in future, depending upon organisation's choice.**	
4.	The Firewall appliance should not be more than 2U rack-mounted design and must have redundant hot swappable power supply to remove any single point of failure.	
5.	The Firewall appliance must deliver 15 Gbps NGFW throughput with Security features (FW, IPS, and Application Control) enabled and 10 Gbps Threat Prevention throughput. The same must be available in the public datasheet.	
6.	The Firewall appliance must deliver 50 Gbps of IPSEC VPN throughput from day 1 without any limitation of VPN Clients.	

7.	The Firewall appliance must deliver 650K new connections/sessions per sec and 50 million concurrent connections/sessions from day1.	
8.	The Firewall appliance must have the security features including IPS, Application Awareness, Anti-Bot, DOS prevention, URL filtering, Anti-Malware, AETs including routing features to be managed from the Central console, no need for any configuration via appliance GUI and Appliance CLI. Solution also support integration with Snort.	
9.	The Firewall appliance must support L3 protocol functionality like Static & policy-based routing, static multicast routing, dynamic routing like MP-BGP, RIPng, OSPF(v2 & v3), IGMP proxy, BGP, BFD, PIM (SM & SSM), and Application-aware routing	
10.	The Firewall appliance must support IPv4 and IPv6 from day 1 with NAT66, NAT64, NAT46 and PAT from day 1	
11.	The Firewall appliance must support IPv6 capability including Dual stack IPv4/IPv6, ICMPv6, DNSv6, IPv6 static, SLAAC, DHCPv6 relay	
12.	The Firewall appliance must support TLS 1.3 and TLS/SSL server certificate verification before decryption decision is taken	
13.	The Firewall appliance must support security proxies for the following TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS	
14.	The Firewall appliance must have Firewall for stateful blocking, URL filtering, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections	
15.	The solution must support client-based agent to check the security posture of endpoints and must be able to employ policies basis the attributes. Policy must be defined on NGFW for discarding the user requests if AV is not updated, OS version is Obsolete, Load on Endpoint is high / any users is using the obsolete browsers and should not have any dependencies on the number of clients supported & there should not be any license attached to it.	
16.	The solution must support high availability and load balancing between multiple ISPs, including VPN connections, Multi-Link VPN link aggregation, QoS-based link selection and admin should be able to manipulate the sensitivity of an application based on jitter, packet loss & latency	
17.	The solution must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active software or configuration.	

18.	The Firewall appliance inspection engine must deliver more than 10000 fingerprint/vulnerabilities for detecting exploit attempts against known vulnerabilities in protocol specific tcp/udp port number. Solution must provide multi-layer inspection to increase network security and performance and it should combine access control to define policies that govern your user's access to network resources, deep inspection to detect advanced threats & file filtering to block malicious file transfers.	
19.	The solution must support 7000+ Applications for better control and visibility throughout the environment so that solution should be able to understand applications like 4sync,4tube, bizible, Facebook, YouTube etc. and should support QUIC & HTTP/3	
20.	The Firewall appliance Inspection Engine/ Anti-Bot must employ the below inspection technologies 1. Multilayer traffic normalization 2. Vulnerability-based fingerprints 3. Evasion and anomaly logging 4. Decryption-based detection 5. Message length sequence analysis	
21.	The solution must support FTP and DNS Proxy to restrict the types of traffic and the commands that can be used with DNS and FTP connections. Solution must support DNS sink holing for UDP and TCP service.	
22.	The solution must provide steering of applications dynamically & should provide application identification with link monitoring to effectively allocate networking resources, ensuring that the critical applications receive the necessary resources for optimal performance.	
23.	The solution must have the technique for monitoring the application health and provide visibility into the organization's network traffic and the administrators should be able detect and resolve bottlenecks before they become a network-wide problem & should provide real-time visibility, historical views, and easy access to connectivity logs directly from the OEM Centralized management dashboard.	
24.	The solution should have an option to create alternative policies if the connectivity between the NGFW and central Manager is lost; any policy should be allowed to be selected whether it is a normal policy or one of the alternative policies	
25.	The solution must prevent against the websites via URL filtering that mask their identity using Dynamic DNS services, Elevated exposure by website that camouflage their true nature, domain name that are registered recently, parked domain, Unauthorized Mobile Marketplaces to prevent users visiting the websites that may distribute applications unauthorized by the mobile OS manufacture	

26.	Solution must be able to prevent the users to visit the websites that use technologies that alter the operation of a user's hardware, software, or network to decrease owner's control with the intent to gain fraudulent access and with potential malicious intent.	
27.	Solution must be able to prevent the users to visit the websites that enable download of software applications or file download servers, download of media content, client software to enable peer-to-peer file sharing and transfer, Sites that store personal files on web servers for backup or exchange.	
28.	Solution should support Re-authentication when using browser-based user authentication and support 4096-bit RSA key for Browser Based User Authentication.	
29.	The solution must have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and blocks access to known malicious sites and non-existent IP addresses with ability to proactively measure against command and control (C2) access & second-stage malware downloads for disrupting the communication between infected endpoints and attackers	
30.	The solution must provide visibility into application health history along with health status history of network applications.	
31.	Solution should have more than 95 URL categories and should support more than 50 languages for better and effective web controls.	
32.	Solution must support File Filtering via Policy for minimum 200 file types in 15 categories and also support file Reputation checking & blocking for file with Malware reputation	
33.	The solution must support custom script upload via Centralize manager so that same script can be used on multiple NGFW and it should support using FQDN to connect between the Firewall and management server & Log Server.	
34.	The solution must support minimum 2000 devices management capability along with SDWAN function and Multi-Layer Traffic Normalization/Full-Stream Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic (both TLS 1.2 and 1.3), Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti-Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods, Automatic Updates	
35.	The management platform must be a dedicated OEM appliance/software/VM running on server and should be capable of managing all the firewalls from day 1 and should be scalable for upto 100 firewalls.	

36.	The solution should come with a web-based administration interface in the dedicated centralized manager and must be able to define the custom roles in addition to predefined roles (e.g., Owner, Viewer, Operator, Editor, Super User) to control permissions flexibly and accurately.	
37.	The centralized management platform must be sized for handling all the managed firewall logs but should not have any licensing limitation on logs per day. Management and log server should have minimum 16 cores, 32 GB RAM with 2 TB log storage capacity.	
38.	Solution should support local user creation options via Central Manager and also support the use of external CA issued certificates in internal management communication and Centralized manager should support to block the access temporarily after multiple failed logon attempts from the same IP.	
39.	The solution must have the ability to support high availability of different model /appliances and versions within the same HA cluster	
40.	The OEM should have presence in India for last 15 years or more and must have Support Center and Registered Office in India to provide sales and support.	
41.	Firewall supports traffic blocking based on custom IP ranges, individual IPs, IP lists, and domain lists. It can integrate with third-party (NTRO, Cert-IN etc) threat intelligence feeds and apply custom URL category filtering.	
42.	VRF supported	

3. Detailed specifications for 48 Port L3 Core Switches

Sl. No	Specifications - 48x 10/25G Port Core Switch
1.	The Switch should support line rate & non-blocking Layer 2 switching and Layer 3 routing
2.	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy and must be hot swappable.
3.	Switch should support the complete STACK of IP V4 and IP V6 services.
4.	Switch should have the following interfaces: 48* 1/10/25G SFP ports & 4 * 40/100GbE QSFP uplink ports populated with 2x 100G 5-meter DAC
5.	Switch should support IEEE Link Aggregation for redundancy across two switches in active- active mode
6.	The switch should support 200k IPv4 routes or above
7.	The switch should support hardware-based load balancing at wire speed using LACP and multi chassis ether channel/LAG
8.	Switch should support minimum 2 Tbps of throughput capacity
9.	Switch should support minimum 250,000 no. of MAC addresses
10.	Switch should support Jumbo Frames up to 9K Bytes on all Ports

11.	Device should support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2
12.	Device Should support graceful restart for BGP, OSPF v2 and v3 and ISIS
13.	Switch should support Policy Based Routing & NAT
14.	Switch should have minimum 16 GB RAM/Memory & Minimum 32 GB Flash/SSD
15.	Switch should provide multicast traffic reachable using:
16.	a. PIM-SM
17.	b. PIM-SSM
18.	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)
19.	e. IGMP V.2 and V.3
20.	Switch should support Multicast routing
21.	Switch Should support BFD inclusive of BFD for Lag links, BFD for V4 and V6 VRF, Multi-hop BFD and BFD on IP unnumbered interfaces.
22.	Switch should support VXLAN with EVPN control plane
23.	Switch must support symmetric VXLAN integrated routing and bridging with EVPN active- active multihoming support.
24.	Switch must support EVPN routes to let hosts connect a specific multicast group.
25.	Switch must support EVPN route type to avoid any sub-optimal routing of the multicast frames across different tenant systems or bridge domains.
26.	Should support 8 queues per port, priority queuing, round-robin queuing
27.	Should support QoS classification, policing and shaping, DSCP and COS.
28.	Should support WRED, Explicit Congestion Notification, priority flow control, data center bridging exchange.
29.	The Device should automatically mirror traffic queued in event of congestion/latency or micro burst and send mirrored traffic to CPU, directly connected server and remote server as per use case.
30.	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
31.	Switch should support for external database for AAA using:
32.	a. TACACS+
33.	b. RADIUS
34.	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
35.	Switch should support MAC ACLs
36.	Should support Standard & Extended ACLs using L2, L3 and L4 fields
37.	Switch should support minimum IEEE 1588 PTP boundary clock mode
38.	Should support telnet, ssh, https, SNMPv3, TWAMP, event manager, scheduler and configuration rollback for ease of operations and management
39.	Switch should support real-time logging of changes in the resource tables like MAC address table, ARP table and route table for monitoring purpose.
40.	The switch should have first hop router redundancy functionality where multiple switches can be configured to provide active/active unicast IP routing such that all the switches respond to the ARP and GARP for the same VLAN virtual IP.
41.	Device Should support Accumulated IGP Metric (AIGP), BGP Monitoring Protocol (BMP) and BGP Prefix Origin Validation with Resource Public Key Infrastructure (RPKI)

42.	device should support on-device execution of python script, bash script and docker containers for automation and programmability support
43.	Switch should support onboard Packet Capture using Wireshark/tcpdump in real time for traffic analysis and fault finding
44.	All relevant licenses for all the above features and scale should be quoted along with switch
45.	Should have hot swappable and field replaceable internal redundant power supply and FAN from day one, should be provided with AC power supply and India power cords.
46.	All licenses should be provided with the devices for the mentioned features.
47.	Visibility & Automation: All Switches & Routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, Multicast Table, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software, if any OEM wants to supply their Appliance they allowed to in HA Cluster
48.	Device should be IPv6 Certified/IPv6 logo ready
49.	Device shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or EN 61000-3-3 Standards for Safety requirements of Information Technology Equipment.
50.	The Device/Device OS should be EAL 3/NDPP/NDcPP certified under Common Criteria.
51.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted as per Hardware WARRANTY AND Software Support clause defined in point M of this document along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature lic should be supplied from Day 1. Hardware & Software Support as per Hardware WARRANTY AND Software Support clause defined in point M of this document.
52.	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.
53.	All Network Switches as part of this Tender should be able to viewed in Single Dashboard.
54.	All Network switches should from Same OEM, for better support and no compatibility issue come up at later stage
55.	All Network Switches should run on same OS for simplified operations.
56.	All Network Switches & Router should be from Same OEM
57.	All Network Switches & Router quoted Models should have support life of 8 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF.
58.	Manufacturer Authorization is Required. Specification mentioned are minimum and any OEM/SI can quote higher specifications.
59.	VRF Supported
60.	SNMP Supported
61.	Netflow Supported

4. Detailed specifications of 48 Port Distribution Switches

Sl. No	Specifications - 48x 10G Port Distribution Switch
1.	The Switch should support line rate & non-blocking Layer 2 switching and Layer 3 routing
2.	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy and must be hot swappable.
3.	Switch should support the complete STACK of IP V4 and IP V6 services.
4.	Switch should have the following interfaces: 48* 1/10G SFP ports & 8/12 * 40/100GbE QSFP uplink ports populated with 2x 100G 5 meter DAC
5.	Switch should support IEEE Link Aggregation for redundancy across two switches in active- active mode
6.	The switch should support 128k IPv4 routes or above
7.	The switch should support hardware-based load balancing at wire speed using LACP and multi chassis ether channel/LAG
8.	Switch should support minimum 2.56 Tbps of throughput capacity
9.	Switch should support minimum 250,000 no.of MAC addresses
10.	Switch should support Jumbo Frames up to 9K Bytes on all Ports
11.	Device should support Routing Protocols: OSPFv2 with multiple instances, OSPFv3, BGP, MP-BGP, IS-IS, and RIPv2
12.	Device Should support graceful restart for BGP, OSPF v2 and v3 and ISIS
13.	Switch should support Policy Based Routing & NAT
14.	Switch should have minimum 16 GB RAM/Memory & Minimum 32 GB Flash/SSD
15.	Switch should provide multicast traffic reachable using:
16.	a. PIM-SM
17.	b. PIM-SSM
18.	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)
19.	e. IGMP V.2 and V.3
20.	Switch should support Multicast routing
21.	Switch Should support BFD inclusive of BFD for Lag links, BFD for V4 and V6 VRF, Multi-hop BFD and BFD on IP unnumbered interfaces.
22.	Switch should support VXLAN with EVPN control plane
23.	Switch must support symmetric VXLAN integrated routing and bridging with EVPN active- active multihoming support.
24.	Switch must support EVPN routes to let hosts connect a specific multicast group.
25.	Switch must support EVPN route type to avoid any sub-optimal routing of the multicast frames across different tenant systems or bridge domains.
26.	Should support 8 queues per port, priority queuing, round-robin queuing
27.	Should support QoS classification, policing and shaping, DSCP and COS.
28.	Should support WRED, Explicit Congestion Notification, priority flow control, data center bridging exchange.

29.	The Device should automatically mirror traffic queued in event of congestion/latency or micro burst and send mirrored traffic to CPU, directly connected server and remote server as per use case.
30.	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
31.	Switch should support for external database for AAA using:
32.	a. TACACS+
33.	b. RADIUS
34.	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
35.	Switch should support MAC ACLs
36.	Should support Standard & Extended ACLs using L2, L3 and L4 fields
37.	Switch should support minimum IEEE 1588 PTP boundary clock mode
38.	Should support telnet, ssh, https, SNMPv3, TWAMP, event manager, scheduler and configuration rollback for ease of operations and management
39.	Switch should support real-time logging of changes in the resource tables like MAC address table, ARP table and route table for monitoring purpose.
40.	The switch should have first hop router redundancy functionality where multiple switches can be configured to provide active/active unicast IP routing such that all the switches respond to the ARP and GARP for the same VLAN virtual IP.
41.	Device Should support Accumulated IGP Metric (AIGP), BGP Monitoring Protocol (BMP) and BGP Prefix Origin Validation with Resource Public Key Infrastructure (RPKI)
42.	device should support on-device execution of python script, bash script and docker containers for automation and programmability support
43.	Switch should support onboard Packet Capture using Wireshark/tcpdump in real time for traffic analysis and fault finding
44.	All relevant licenses for all the above features and scale should be quoted along with switch
45.	Should have hot swappable and field replaceable internal redundant power supply and FAN from day one, should be provided with AC power supply and India power cords.
46.	All licenses should be provided with the devices for the mentioned features.
47.	Visibility & Automation: All Switches & Routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, Multicast Table, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software, if any OEM wants to supply their Appliance they allowed to in HA Cluster
48.	Device should be IPv6 Certified/IPv6 logo ready
49.	Device shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or EN 61000-3-3 Standards for Safety requirements of Information Technology Equipment.
50.	The Device/Device OS should be EAL 3/NDPP/NDcPP certified under Common Criteria.

51.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted as per Hardware WARRANTY AND Software Support clause defined in point M of this document along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature should be supplied from Day 1. Hardware & Software Support as per Hardware WARRANTY AND Software Support clause defined in point M of this document.
52.	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.
53.	All Network Switches as part of this Tender should be able to viewed in Single Dashboard.
54.	All Network switches should from Same OEM, for better support and no compatibility issue come up at later stage
55.	All Network Switches should run on same OS for simplified operations.
56.	All Network Switches & Router should be from Same OEM
57.	All Network Switches & Router quoted Models should have support life of 8 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF.
58.	Manufacturer Authorization is Required. Specification mentioned are minimum and any OEM/SI can quote higher specifications.
59.	VRF Supported
60.	SNMP Supported
61.	Netflow Supported

5. Detailed specifications for Access Layer Switch (L2 Cluster)

S No.	Specification - 48 Port Switch
A.	**Hardware Specifications**
1.	Device should have 48* 100M/1G RJ45 Ports and 4x 1/10G or better Uplink Ports in 1 RU fixed Form Factor
2.	Device should have total Throughput of 296 Gbps.
3.	Device should support copper Base-T (1G) connectivity over CAT6 cable and 1G, Dual rate 1G/10G SFP+ fiber connectivity over MM and SM cable for the Uplink ports.
4.	Device should support upto 64K MAC address
5.	Device should support upto 8K IPv4 and 2k IPv6 routes simultaneously
6.	Device should have 1G management port, USB port and console port
B.	**L2 features**
7.	Device should support 4K VLANs, 9K Jumbo frame
8.	Device should support MST, per-vlan, RSTP, BPDU Guard, Loop Guard
9.	Device support LLDP, LLDP-MED and LACP to bundle links and detect mis cabling issues.
10.	Device Should support IEEE 802.1D, 802.1Q, 802.1w, 802.1s, 802.3x and 802.1x and Q-in-Q

11.	Switch Should support BFD inclusive of BFD for Lag links, Multi-hop BFD and BFD on IP unnumbered interfaces.
C.	**L3 features**
12.	Device should support Routing Protocols: OSPFv2 with multiple instances, ISIS, OSPFv3, BGP, MP-BGP, RIPv2, BFD
13.	Device should support IGMP v2/v3, PIM-SM, Anycast RP (RFC 4610)
14.	Device Should support 16-way ECMP, VRRP V4 and V6 and must be IPv6 ready.
15.	Device should support Vx LAN+ EVPN from Day 1
16.	Vx LAN+ EVPN should be deployed on IEEE Open Architecture
D.	**High availability**
17.	Device should have N+1 redundant Fans & N + 1 redundant power supply
18.	**Security**
19.	Should support Storm control and Control Plane protection (CPP), ACL with l2, L3 and L4 parameters upto 2K ACLs
20.	Device should support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, named VLAN assignment and priority between 802.1x and Mac based authentication
E.	**Management**
21.	Device Should support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.
22.	Should support real time state streaming telemetry for advance monitoring from day 1
23.	Should Support industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.
24.	Should support NTP, PTP, PFC & ECN
25.	should support SNMP v1/2/3 and Open Configuration model over gRPC/Netconf
26.	Device should support real time data collection with sflow/netflow
27.	Should support recording changes in hardware resource tables like MAC table, Multicast Table, ARP table, IPv6 neighbour table, IPv4 route table, IPv6 route table, etc for troubleshooting & monitoring purpose
F.	**Automation & Visibility**
28.	Device should support multiple simultaneous mirroring sessions across all ports.
29.	Should have programmability and automation support with on board python and bash
30.	Solution should be provided for centralized administration/Management/Control of Switches. Solution should support real-time Telemetry function where in it should receive telemetry information from the switches.
31.	Visibility & Automation: All Switches & routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software, if any OEM wants to supply their Appliance they allowed to in HA Cluster
32.	Should support 8 queues per port, priority queue
33.	Should support Weighted Fair Queue or Weighted round robin or equivalent
34.	Should support ACL based classification for QoS, rate limiting function like policing and shaping

G.	**Others**
35.	Switch or Switch OS should be EAL2/EAL3/NDPP / NDcPP certified.
36.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted with as per Hardware WARRANTY AND Software Support clause defined in point M of this document along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature should be supplied from Day 1. Hardware & Software Support as per Hardware WARRANTY AND Software Support clause defined in point M of this document.
37.	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.
38.	All Network Switches & Routers quoted Models should have support life of 8 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF.
39.	Manufacturer Authorization is Required. Specification mentioned are minimum and any OEM/SI can quote higher specifications.
40.	All Network Switches & Router as part of this Tender should be able to viewed in Single Dashboard.
41.	All Network switches & Routers should from Same OEM, for better support and no compatibility issue come up at later stage
42.	All Network Switches & Routers should run on same OS for simplified operations.
43.	VRF Supported
44.	SNMP Supported
45.	Netflow Supported

6. Detailed Specifications for OOB/ Management Switch 48 Port

S No.	Specification - 48 Port Switch
A.	**Hardware Specifications**
1.	Device should have 48* 100M/1G RJ45 Ports and 4x 10/25G or better Uplink Ports in 1 RU fixed Form Factor
2.	Device should have total Throughput of 176 Gbps.
3.	Device should support copper Base-T (1G) connectivity over CAT6 cable and 1G, Dual rate 1G/10G SFP+ fiber connectivity over MM and SM cable for the Uplink ports.
4.	Device should support upto 64K MAC address
5.	Device should support upto 8K IPv4 and 2k IPv6 routes simultaneously
6.	Device should have 1G management port, USB port and console port
B.	**L2 features**
7.	Device should support 4K VLANs, 9K Jumbo frame
8.	Device should support MST, per-vlan, RSTP, BPDU Guard, Loop Guard
9.	Device support LLDP, LLDP-MED and LACP to bundle links and detect miscabling issues.
10.	Device Should support IEEE 802.1D, 802.1Q, 802.1w, 802.1s, 802.3x and 802.1x and Q-in-Q

11.	Switch Should support BFD inclusive of BFD for Lag links, Multi-hop BFD and BFD on IP unnumbered interfaces.
C.	**L3 features**
12.	Device should support Routing Protocols: OSPFv2 with multiple instances, ISIS, OSPFv3, BGP, MP-BGP, RIPv2, BFD
13.	Device should support IGMP v2/v3, PIM-SM, Anycast RP (RFC 4610)
14.	Device Should support 16-way ECMP, VRRP V4 and V6 and must be IPv6 ready.
15.	Device should support VxLAN+EVPN from Day 1
16.	VxLAN+EVPN should be deployed on IEEE Open Architecture
D.	**High availability**
17.	Device should have N+1 redundant Fans & N + 1 redundant power supply
E.	**Security**
18.	Should support Storm control and Control Plane protection (CPP), ACL with l2, L3 and L4 parameters upto 2K ACLs
19.	Device should support IEEE 802.1x Authentication framework, MAC authentication, Dynamic VLAN assignment, named VLAN assignment and priority between 802.1x and Mac based authentication
F.	**Management**
20.	Device Should support secure Zero touch provisioning with options to provision Certificates artifacts on the device when it boots.
21.	Should support real time state streaming telemetry for advance monitoring from day 1
22.	Should Support industry standard hierarchical CLI, SSHv2, HTTPS, SCP, SFTP, CLI task scheduler and configuration session.
23.	Should support NTP, PTP, PFC & ECN
24.	should support SNMP v1/2/3 and OpenConfig model over gRPC/Netconf
25.	Device should support real time data collection with sflow/netflow
26.	Should support recording changes in hardware resource tables like MAC table, Multicast Table, ARP table, IPv6 neighbour table, IPv4 route table, IPv6 route table, etc for troubleshooting & monitoring purpose
G.	**Automation & Visibility**
27.	Device should support multiple simultaneous mirroring sessions across all ports.
28.	Should have programmability and automation support with on board python and bash
29.	Solution should be provided for centralized administration/Management/Control of Switches. Solution should support real-time Telemetry function where in it should receive telemetry information from the switches.
30.	Visibility & Automation: All Switches & routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution from the same OEM. Should support telemetry with time-series database view, traffic flow analytics, PSIRT/BUG visibility, configuration compliance, endpoint tracking, POAP/ZTP, device resource utilization, auto topology view, alerts. SI will factor required VM's to install the software, if any OEM wants to supply their Appliance they allowed to in HA Cluster
31.	Should support 8 queues per port, priority queue
32.	Should support Weighted Fair Queue or Weighted round robin or equivalent
33.	Should support ACL based classification for QoS, rate limiting function like policing and shaping
H.	**Others**

34.	Switch or Switch OS should be EAL2/EAL3/NDPP / NDcPP certified.
35.	Hardware replacement warranty and TAC support should be directly from the OEM. OEM email-id and India Contact support no. to be provided. The Switching System shall be quoted as per Hardware WARRANTY AND Software Support clause defined in point M of this document along with OEM web based / telephonic technical Support. The same shall be verifiable on OEMs website. All asked feature lic should be supplied from Day 1. Hardware & Software Support as per Hardware WARRANTY AND Software Support clause defined in point M of this document.
36.	OEM & Bidder shouldn't be from a country which shares a land border with India and Hardware shouldn't be Manufactured & Assembled from a country which shares a land border with India. Same should be declared in MAF.
37.	All Network Switches & Routers quoted Models should have support life of 8 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF.
38.	Manufacturer Authorization is Required. Specification mentioned are minimum and any OEM/SI can quote higher specifications.
39.	All Network Switches & Router as part of this Tender should be able to viewed in Single Dashboard.
40.	All Network switches & Routers should from Same OEM, for better support and no compatibility issue come up at later stage
41.	All Network Switches & Routers should run on same OS for simplified operations.

7. Detailed Specifications for Silver Grade 2 Socket Server, 32 Cores 512 GB RAM

S. No.	Parameter	Specifications/ Values	Remarks
1.	Processor Configuration	2x Intel Xeon Silver CPUs (min 16 cores each)	
2.	Total Number of Cores	32 physical cores minimum	
3.	Threads	≥64 threads (with HT)	
4.	Memory Configuration	512 GB DDR5 RDIMM ECC (scalable up to 1 TB or more)	
5.	Memory Speed	Minimum 4800 MT/s (DDR5)	
6.	Storage Bays (Hot-Swap)	Min. 8x 2.5" or 3.5" SAS/SATA/NVMe hot-swappable bays	
7.	RAID Support	Hardware RAID (RAID 0, 1, 5, 10) with battery-backed cache	Hardware RAID (RAID 0, 1, 5, 10) with 8GB NV cache
8.	Storage	Required total HDD capacity 12 TB	Required total HDD capacity 12 TB using SAS 10k RPM drive
9.	Networking	6 x 1G Ethernet (on-board + PCIe based), 1x 10G (SFP+) along with module	6 x 1G Ethernet ports (on-board + PCIe based), 1x 10G (SFP+) ports along with module
10.	PCIe Expansion Slots	Min. 3 PCIe Gen4 slots	
11.	Management	Dedicated management port with IPMI/iLO/iDRAC	Dedicated management port and management software

12.	Remote Console Access	Web-based full remote console & media mounting support	Management Adaptor should provide User Interfaces such as: HTML5 Web, Redfish, WSMAN IPMI 2.0, DCMI 1.5, RACADM, SSH, Serial Console Redirection to configure Full BIOS over 50 BIOS Features. Management Adaptor should enable Chat enabled remote virtual console sharing up to 6 users simultaneously during pre-OS and OS runtime operation
13.	Power Supplies	Dual hot-swappable redundant Platinum-certified PSUs	
14.	Form Factor	2U Rack-mountable	
15.	Firmware Security	Secure Boot, TPM 2.0, UEFI, BIOS recovery, silicon root of trust	Secure Boot, TPM 2.0, UEFI, BIOS recovery, silicon root of trust. Cryptographically verified trusted booting standards meeting basis NIST SP 800-147B, BIOS Integrity measurement proposed guidelines basis NIST SP 800-155, protection standards meeting NIST SP 800-193 and standards & secure media sanitization standards meeting NIST SP 800-88.
16.	Operating System Support	RHEL, CentOS, Windows Server, VMware, Ubuntu	
17.	Certifications	BIS, FCC, CE, UL, RoHS, ISO 9001	
18.	Support		Comprehensive support with defective component retention as per Hardware WARRANTY AND Software Support clause defined in point M of this document. In case of failure no component will be returned against replacement like but not limited to HDD, RAM, Motherboard, RAID controller, Network card or any other component may have any confidential/crucial information.

8. Detailed Specifications for Silver Grade 2 Socket Server, 16 Cores 128 GB RAM

S. No.	Parameter	Specifications/ Values	Remarks
1.	Processor Sockets	2x CPU sockets with support for Intel Xeon Silver series	
2.	Total CPU Cores	Minimum 16 physical cores (e.g., 2×8 cores or 1×16 cores)	
3.	Memory (RAM)	128 GB DDR4 or DDR5 ECC Registered RAM, scalable to ≥1 TB	
4.	Memory Scalability	Minimum 1 TB (via additional DIMM slots)	
5.	Storage Bays	Minimum 8x 2.5" or 3.5" hot-swappable drive bays (SAS/SATA/NVMe)	
6.	Storage Controller	RAID controller with RAID 0, 1, 5, 10 support	Hardware RAID (RAID 0, 1, 5, 10) with 8GB NV cache
7.	Storage	Required total HDD capacity 12 TB	Required total HDD capacity 12 TB using SAS 10k RPM drive
8.	Networking	2x 1GBase-T onboard + 1x 10G optional (SFP+/RJ45)	2x 1GBase-T ports onboard + 2x 10G SFP+ ports along with modules
9.	Expansion Slots	Minimum 3x PCIe Gen4 slots	
10.	Management	Dedicated management port with IPMI/iLO/iDRAC	Dedicated management port and management software
11.	Remote Management	Dedicated out-of-band port with HTML5/iKVM (IPMI, Redfish, etc.)	Management Adaptor should provide User Interfaces such as: HTML5 Web, Redfish, WSMAN IPMI 2.0, DCMI 1.5, RACADM, SSH, Serial Console Redirection to configure Full BIOS over 50 BIOS Features. Management Adaptor should enable Chat enabled remote virtual console sharing up to 6 users simultaneously during pre-OS and OS runtime operation
12.	Power Supply Units (PSU)	Redundant, hot-swappable 500W–800W PSUs (80 PLUS Platinum/Gold)	Dual hot-swappable redundant Platinum-certified PSUs
13.	Form Factor	2U rack-mountable	
14.	Operating Temperature Range	10°C to 35°C	
15.	Security Features	TPM 2.0, Secure Boot, Silicon Root of Trust	Secure Boot, TPM 2.0, UEFI, BIOS recovery, silicon root

			of trust. Cryptographically verified trusted booting standards meeting basis NIST SP 800-147B, BIOS Integrity measurement proposed guidelines basis NIST SP 800-155, protection standards meeting NIST SP 800-193 and standards & secure media sanitization standards meeting NIST SP 800-88.
16.	Supported OS	Windows Server, RHEL, Ubuntu, VMware ESXi	
17.	Certifications	RoHS, CE, FCC Class A, UL, ISO 9001	
18.	Support		Comprehensive support with defective component retention as per Hardware WARRANTY AND Software Support clause defined in point M of this document.. In case of failure no component will be returned against replacement like but not limited to HDD, RAM, Motherboard, RAID controller, Network card or any other component may have any confidential/crucial information.

OS disk of 480 GB SSD or higher. All VM and workload data, apart from the OS disk, will be centrally stored on SAN storage. Additionally, internal extra storage will be provisioned for the Rsyslog server to store logs from NAFIS, CCTNS, and I-MOT.

9. Detailed specifications for 400TB NAS Appliance (10TB Hot/ 390TB cold) RAID 6

S. No.	Parameter	Specifications/ Values	Remarks
1.	Total Usable Capacity	≥ 400 TB usable (10TB hot, 390TB cold)	
2.	RAID Support	Must support RAID 6 (or equivalent N+2 protection)	
3.	Scalability	Must support scaling to at least 1 PB within same family	
4.	Drive Types Supported	SAS/NL-SAS/SSD based on tier (SSD+SAS for Hot, NL-SAS for Cold)	

S. No.	Parameter	Specifications/ Values	Remarks
5.	Storage Protocols	NFS v3/v4, SMB v2/v3, FTP, SFTP, HTTP, NDMP	
6.	Access Method	NAS (file-level); unified namespace	
7.	Throughput (Hot Tier)	Minimum 5 Gbps aggregate read/write	
8.	Data Tiering Support	Automated policy-based tiering between hot/cold	
9.	Snapshot & Backup Support	Support for snapshotting, cloning, deduplication, and backup integration	
10.	File System Features	Distributed File System, journaling, metadata replication	
11.	Authentication Integration	LDAP, AD, NIS, Kerberos	
12.	Network Interfaces	Minimum 4x 10GbE ports per node; LACP/port channel support	
13.	Power Redundancy	Dual redundant hot-swappable power supplies	
14.	Management Interface	Web GUI, CLI, REST API, SNMP	
15.	Rack Mounting	2U/4U rack-mount chassis with rails	
16.	Monitoring & Alerts	SNMPv3, email alerting, integration with SIEM	
17.	Compliance Standards	RoHS, UL, CE, ISO 27001 readiness	

10. Detailed specifications of 500 TB Object Storage for backup

S. No.	Parameter	Specifications/ Values	Remarks
1.	Total Usable Capacity	Minimum 500 TB usable (scalable to multi-PB)	
2.	Hot Tier Capacity	Minimum 50 TB of high-performance object storage	
3.	Cold Tier Capacity	Minimum 200 TB cold/archival storage	
4.	Object Protocol Support	Must support S3, OpenStack Swift, and optionally NFS/SMB	
5.	Scalability	Horizontal scaling up to multiple petabytes	
6.	Storage Architecture	Software-defined object storage with erasure coding & replication	
7.	Throughput (Hot Tier)	≥ 10 GB/s aggregate throughput for hot-tier access	
8.	Latency (Hot Tier)	≤ 10ms average write latency (hot tier)	
9.	Data Durability	≥ 99.999999999% (11 nines)	
10.	Data Availability	≥ 99.999%	
11.	Multi-Tenancy Support	Native multi-tenant, secure namespace isolation	
12.	Retention & Compliance	WORM, Legal Hold, Retention Policies, Audit Logging	

S. No.	Parameter	Specifications/ Values	Remarks
13.	Backup Integration	Should integrate with industry backup software (Commvault, Veeam, etc.)	
14.	Encryption	AES-256 at rest, TLS 1.2+ in transit	
15.	Management Interface	Web GUI + REST API + CLI	
16.	Monitoring & Alerts	SNMP, Syslog, Prometheus, Role-based Dashboards	
17.	Power and Cooling	Redundant PSUs, typical 2–3 kW/rack for hot+cold tier	
18.	Rack Form Factor	4U or 5U node-based appliance enclosure	
19.	Compliance Certifications	FIPS 140-2, ISO 27001, Common Criteria preferred	

11. Detailed Specifications of SIEM 10000 EPS

Security Incident and Event Management (SIEM)		Bidder Compliance (Yes / No)
Sl. No	Specifications	
1.	SIEM solutions must be dedicated on premise solutions. The Bidder should propose the necessary hardware along with any additional software licences (Database, Virtualization, etc) as part of the proposal.	
2.	The solution must provide the ability to encrypt communications on the network between SIEM components and SIEM	
3.	The solution must ensure all distributed system components continue to operate when few parts of the NG-SOC solution fail or loses connectivity (i.e. management engine goes off-line; all separate collectors continue to capture logs).	
4.	The solution should allow a wizard-based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules	
5.	Collection, Correlation and Console layer should be logically separate.	
A.	Log Management	
6.	The SIEM should support a 10000 EPS or higher at all layers from day one. It should be able to handle a burst of 1.25 times of the given EPS in real time at any given point in time without any drop or queuing of events. The Solution should be scalable to up-to 11000 EPS or higher within the same hardware.	
7.	Raw and normalized Logs should be handled and stored in tamper proof way across SIEM solution. alter/modify tamper rights w.r.t Raw logs. The solution must provide capabilities for time stamping, efficient storage and compression (minimum 20%) of collected data.	
8.	The proposed solution should be able to pull the logs through JDBC & ODBC connectors out of the box	

9.	The solution should have customizable parsers to accept and process unknown log formats. Raw logs should be visible to the user in one single click. Raw log data from the solution shall be made downloadable without the need of OEM dependent tools.		
10.	The proposed SIEM solution should highlight the number of parsed/unparsed logs per hour for each sub organisations		
11.	The solution should have live visualization of logs received from each source. Should have dedicated dashboards for each sub organization and log sources.		
12.	Log Search Interface: The proposed solution must provide a simple, intuitive search interface using following search methodologies: a) Search Templates b) Search Patterns c) Search Operators d) Search Export e) Search Criteria f) Search Time Range g) Search Results View		
13.	The solution must have the capability of Multi tenancy and should support a minimum of 10 tenants in the same system. The solution should have RBACs in place to limit the tenant level visibility.		
14.	Log Management Automation: The proposed solution must provide a log management solution and must retain a minimum of 90 days of data retention online and 1 year of archival support. And these logs should be readily accessible, However, if the owner wishes to store online logs for more duration.		
15.	Universal Log Analysis: The proposed solution must contain system content that can be used for cyber-security, compliance, application and IT & OT operations monitoring and must support additional content specific to regulations like ISO 27001, IT-Act etc..		
16.	Log Data Integrity: The proposed solution must provide audit trail of all the administration activities such as login, logouts, new user creations, etc		
17.	The proposed solution search performance must be capable of searching through millions of structured (indexed) events and unstructured (raw) log messages.		
18.	Retention Policy Suspension: The proposed solution must provide the ability to suspend the retention configurations manually and allow administrators to increase the retention period.		
19.	The solution should be able to conduct agentless collection of logs except for those which cannot publish native audit logs. System should not leverage any open-source agents like OSquery, Wazuh, fluentd etc & instead the agents should be from the same OEM.		
B.	Event & Log Collection		

20.	The solution should be able to collect and process raw logs in real- time from any IP Device including Networking devices (router/switches/voice gateways), Security devices (IDS/IPS, AV, Patch Mgmt, Firewall/DB Security solutions), Operating systems (Windows (all flavors), Unix, LINUX (all flavors), AIX etc), Virtualization platforms, Databases (Oracle, SQL, DB2 etc.), Storage systems, and Enterprise Management systems etc. The list of supported systems with which SIEM can INTEGRATE in each category viz. Network, Security, OS, Databases, Servers, Mainframe, Anti-malware system, Storage, Backup system, Hypervisors.		
21.	The system should support, not restricted to, the following log and event collection methods: ▪ Syslog ▪ Flat file logs such as from DNS, DHCP, Mail servers, web servers etc. ▪ Windows events logs – Agent-based or agent- less. ▪ FTP, S/FTP, SNMP, ODBC, SDEE, WMI, JDBC, etc.		
22.	Categorized Event Data: The proposed solution must categorize log data into an easy-to-understand humanly-readable format that does not require knowledge of OEM-specific event IDs to conduct investigation, define new correlation rules, and/or create new reports/dashboards.		
23.	Reliable Transport: Log Transmission should use reliable TCP protocol that will ensure retransmission in the event of protocol failure to ensure that no log data is lost in transit.		
24.	Collection Health Monitoring: Any failures of the log forwarding must be detected immediately and operations personnel must be notified via communication mediums such as e -mail.		
25.	Caching & Batching: The proposed solution must support local caching and batching at collection level in case of connectivity failures.		
26.	Time Correction: The proposed solution must be capable of collecting event time for systems along with collection time and alerting time. This allows integrity for forensic analysis to determine the original time of the event source and what the system time was for each system component processing the event.		
27.	Centralized Incident Management: The proposed solution must provide an interface to view the incidents and alerts generated. The solution should have integrated Incident review frameworks such as MITRE ATT&CK and Attack Kill Chain integrated.		
28.	Correlation		
29.	Correlation Rules: The proposed solution must provide correlations rules out-of-the-box.		
30.	Cross-Device Correlation: The proposed solution must be capable of correlating activity across multiple devices out-of-the-box to detect authentication failures, perimeter security and operational events in real -time without the need to specify particular device types		

31.	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in five minutes then send a notification.		
32.	The solution must support correlated incidents for applications, databases, servers, networks etc. based on feed from other solutions like PAM, WAF, NBAD, TIP, Threat hunting Centre and UEBA		
33.	The solution must provide many correlations rules out-of-the-box. Again, the option of creating/configuring new rules must be available.		
34.	Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: 1) Vulnerability based 2) Statistical based 3) Signature Based 4) Event Based 5) Unauthorized Access 6) Denial of Service 7) Service Unavailable 8) Whitelist/Blacklist/Reference List		
35.	The solution should have intelligence to extract Information from leading global intelligence sources, proposed threat intelligence platform and use it for valid correlation. Threat Intel should be provided from the OEM itself.		
36.	The solution should be able to collect and store data from various devices as text/csv files and use it for analysis.		
37.	The system should provide adequate categorization and prioritization of the collected and aggregated events from the monitored log sources. This entails a deep understanding of the event types and criticality associated with the events for the supported log sources. The categorization may be HIGH, MEDIUM, LOW or color coding. The dashboard should visualize individual log source wise dashboards.		
38.	The system/solution should have the ability to correlate all the fields in a log.		
39.	Events should not be dropped if it exceeds the EPS limitation for a period of 48 Hrs.		
40.	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc.		
41.	Custom Dashboards: The proposed solution must provide the framework to create custom visual displays to support security operations.		
42.	Dashboard Drill-Down: The proposed solution must provide the ability to allow analysts to drill -down from graphical dashboards to the underlying event data.		
43.	All the latest updates and patches for the solution should be updated to the NG-SOC without any additional cost		

44.	All the Event, Alerts and other information pertaining to Data Centre's NG-SOC must remain within Data Centre premises only. Any information moving out of Data Centre premises shall be reviewed and approved by the Data Centre on need basis.		
45.	Reusable Content: The solution must allow users to create objects such as filters or search queries that are reusable for the ease of operations		
C.	Alerting		
46.	The solution must provide real time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms such as email, sms etc. based on agreed policies.		
47.	Solution must be capable of monitoring attack/incident history against critical assets or by particular users.		
48.	Alert Filters: The proposed solution must provide pre - defined alerts and provide the ability to re-use predefined filters and own created filters as alert criteria		
D.	Reporting		
49.	The solution should showcase the real time logs coming in from each and every source and should have the ability to filter out specific sources and specific keyword-based filters in Realtime data ingestion.		
50.	The solution must provide reporting engine for out-of- box reports, customized reports, ability to schedule reports, compliance reports, historical reports with the following options: 1. Detailed reports of non-compliant activities and policy violations in the network. 2. The solution must provide a reporting engine for out-of-box reports, customized reports, ability to schedule reports, compliance reports etc. 3. The solution should provide out of box templates for reports on ISO, PCI, SOX and other standards. 4. The system should allow scheduling reports. 5. Reports should be available in pdf and csv format.		
E.	Dashboard		
51.	The SIEM solution must provide central management of all components and administrative functions from a single web based / console user interface.		
52.	Customizable Dashboards: The proposed solution should provide dashboards specific to each user and should be user configurable. The dashboards must be capable of displaying multiple daily reports specific to each user's job function.		
53.	SIEM solution should be able to map correlation rules/use cases with MITRE ATT&CK Framework and Cyber Kill Chain for tactics and techniques to get better visibility of incidents and shall be a part of the proposed solution.		

54.	The solution should support customization of inbuilt correlation rules. The solution must allow to build, test, and deploy unlimited custom log parsers and data normalization rules via a self-service graphical interface, without requiring vendor or partner professional services involvement.		
55.	In case the connectivity with the SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.		
56.	The solution should allow creation of custom reporting dashboards from forensics search conducted on the system		
57.	Solution should have an OOTB bidirectional integration with Threat Intel Platform.		
58.	The system should be capable of consuming Threat Intelligence from Third Party sources as well.		
F.	Administration		
59.	The Solution should provide a web-based administration user interface for device management and monitoring.		
60.	Administration Dashboard: The proposed solution must provide a single administrative dashboard to analyze the system load, resource utilization and storage performance trends.		
61.	System Process Status: The proposed solution must provide an administration page that allows viewing underlying system process status and resetting application components without having to restart the entire system. This should be provided through the same web interface along with all other administrative tasks.		
62.	The solution should be multi-tenant with RBAC and should provide dedicated dashboards for the officials		
G.	Threat Hunting Features:		
63.	The solution should have out of the box capability to integrate with CERT-In CMTX threat feeds.		
64.	The solution should give ability to perform open searches with simple and complex queries and enable threat hunting		
65.	The solution should provide ML based detections for Domain Randomness, DNS Fuzzy Matching, Email Fuzzy Matching etc.		
66.	The solution should be capable of supporting AI based Threat Hunting.		
H.	Log Collector		
67.	Should be able to collect logs from all the devices.		
68.	Log collector should also act as a connector for SOAR to take remediation actions and access devices which are behind a firewall.		
69.	The log collector should be able to compress the logs it collects to at least 50% and transmit the logs in an encrypted format.		

70.	The logs collector should have the capability to store logs in case connectivity fails. The collectors should be sized to store at least 5 day's worth of data.	
71.	The log collectors shall use TLS encryption to forward data.	
72.	The log collector shall have inbuilt JDBC & ODBC Connectors for collecting logs from Databases.	
73.	The log collectors should be capable to be deployed in Physical & Virtual Server Environments	
74.	The log collectors should have the ability to collect flows if required.	
75.	The log collectors should have the capability to be deployed in HA.	

12. Detailed specifications of SOAR

Sl. No	SOAR (Security Orchestration, Automated and Response)	Bidder Compliance (Yes / No)
A.	Specifications	
1.	The solution must be a fully on-premise solution deployed in house. The OEM to recommend the sizing for the hardware/VM for the proposed solution	
2.	SOAR should be able to integrate bi-directionally with the SIEM solution being proposed from day 1.	
3.	SOAR platform must have out-of-box or ready integration with the various technologies used in the Owner environment to consume alert data, perform investigative and remediation actions.	
4.	The solution must be able to support creation of incidents via API, Web URL, SIEM, Ticketing system, manually etc.	
5.	Solution supports Integrations with external ticketing platforms.	
6.	The solution must have capability to design workflow to provide fully automated action for the detected incident.	
7.	The solution must have the capability to notify users based on detected/ identified incidents.	
8.	Solution shall have the capability of providing independent threat intelligence for local and external threats.	
9.	The solution should provide for Threat Intelligence and Threat hunting capability via integration with the proposed TIP and Threat hunting platform.	
10.	Any information moving out of the Organization premises shall be reviewed and approved by officials on a need basis.	
11.	Solution should support at least 2 analysts with support for storing up to 5 million indicators in the database from day 1.	
12.	Solution should support Multi Factor Authentication	
13.	The system should support a graphic UI for creations of playbooks. The flow of playbooks should be in form of drag and drop.	

14.	The SOAR capability should include running of custom scripts such as but not limited to bash,python,ruby inside a playbook		
15.	The solution should offer a dedicated SOAR test lab workspace, empowering users to experiment, validate, and enhance automated security workflows in a controlled testing environment		
B.	**Integration**		
16.	Solution should support integration with min 100 third party OEM products including but not limited to the following technologies. > Forensic tools > IT tools (AD, ISE, NOC tools) > Specify all products IT e.g. (AD, SAML) Communication tools (e.g ... Emails, SMS) SIEM tools. > Endpoint Security Solution > Network Security Solution > Threat Intelligence.		
17.	Solution should support adding of new product integrations and custom integrations without any additional cost to SOC. Also, should integrate with existing Incident management tools and IT ticketing system.		
18.	The solution should integrate with partner products using any of the standard protocols and interfaces including REST API, SOAP, SSH/CLI interface, and custom APIs.		
C.	**Automation and Response**		
19.	The solution should provide a simple, comprehensive, fully automated approach to detect and stop the threats that matter, for on premise deployments from internal & external attacks on the IT and OT system.		
20.	The solution should support both human and machine-based automation for various tasks related to security investigations.		
21.	Solution should use playbooks/runbooks with a visual editor/canvas which supports visual creation of playbooks without the need to code by native integration to third party tools and processes.		
22.	Solution should auto remediate the problem without causing a huge impact to the organization. Some of the examples such remediation could be: • Push policies to prevent an external IP • Isolate an internal desktop/Server • Disabling user accounts used for malicious purposes		

	23.	Solution should be configured with the used cases with automation for response to the minimum basic threats like: • Blacklisted IP Communication • Possible Penetration Testing Activity • Connection to Known Malicious Actor in Published Host List • DDOS Attack • Vulnerability scan detection • Phishing detection • Brute force attack • Malware /threat activity monitoring • Ransomware • Buffer Overflow attacks • Port & vulnerability Scans • Worm/virus outbreak • File access failures • Unauthorized server/service restarts • Unauthorized changes to firewall rules		
	24.	Solution should have built in reusable playbooks for well-known Incident types (Phishing, Malware, IOC Hunt).		
	25.	Solution Should allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks. Solution should allow a single playbook to have Automated and Manual Tasks within the same playbook.		
	26.	Solution should allow a complete playbook to be run automatically or manually and list out any exceptions.		
	27.	Solution must support step by step debugging of the running playbooks with provision of starting from where it stopped on error.		
	28.	The proposed SOAR solution should must have out of the capability to extract metadata from emails including Multi-part body, Links present in an email, return path, Subject, Email Body, SMTP server Ip, Email attachment, SMTP Server Domain, IPs present in Email, Domains present in email and allow it to be used for rest of the playbook actions from day one without any third party dependency.		
	29.	Solution should allow addition of adhoc tasks within a playbook.		
	30.	The solution must have an integrated versioning mechanism to save and maintain multiple versions for the playbooks.		
	31.	The solution should not limit the number of SOAR playbooks to be created.		
	32.	The system should support automatic reporting back to ticketing solutions for example for closing cases state. These actions will be added to the audit trail.		
	33.	The solution should be able to consume security alerts/incidents from SIEM or directly from any other IT security solutions.		
	34.	Solution should support email or text notifications, along with functionality to email comprehensive periodic reports and dashboards.		

35.	Solution should provide necessary integration with the IT/cybersecurity systems for keeping the forensics artifacts from the integrated sources of the incident before taking remedial actions.		
D.	**Correlation & Analytics**		
36.	Solution should support assigning of incident to a User.		
37.	Solution should support highlighting of active incidents to quickly identify and access them.		
38.	Solution should support visual mapping of an incident, its elements and correlated investigation entities, and the progression path of the incident.		
39.	Solution should support external users to contribute to an incident via email, message etc.		
40.	System should allow more than 1 playbook to run on any incident. All execution details should be retained and available for the reference.		
41.	Solution should allow differentiation between alerts and incidents (incidents could be made of multiple alerts.)		
42.	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution.		
43.	The system should support creation of an incident based on an email input (e.g. analyze all emails from a dedicated phishing mailbox)		
44.	The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling a rapid and efficient response.		
E.	**Reporting**		
45.	Solution should record timestamp for all actions taken in an incident		
46.	The solution should provide predefined reports and support the creation of customized reports in formats like CSV, DOC, and PDF, including the option to add a custom logo of the organization		
47.	Solution should support Dashboards which can provide high level view of Platform to the management		
48.	Solution should have documentation readily available for using automation and creation of custom automation		
49.	Solution should be able to perform the actions by taking inputs from end user		
F.	**Administration and Configuration**		
50.	The solution must support a web-based GUI for management, analysis and reporting.		
51.	The solution must provide central management of incidents and administrative functions from a single web-based user interface.		
52.	Case Management: The proposed solution must provide a complete process framework for integrating security monitoring and investigations with existing workflow procedures. Workflow should involve escalating an		

	incident to other users within the same team or within other teams etc.	
53.	Incident Tracking: The proposed solution must provide necessary tools to identify, isolate and remediate incidents as they occur.	
54.	The solution should provide a web-based tool for incident management and the same should follow industry best practices	
55.	The administrator must be able to define role-based access to various functional areas of the solution. This includes being able to restrict a user's access to specific functions of the solution that is not within the scope of a user's role including, but not limited to, administration, reporting, incident assignment, playbook creation.	
G.	**Threat Intel Platform**	
56.	SOAR should have an integrated Threat Intelligence Platform (TIP) and should Facilitate importing and parsing structured and unstructured intelligence documents-Structured/finished intelligence analysis reports (.txt); Automatically ingest email lists with threat information; Formatted CSV Files, XML-based structured intelligence – STIX	
57.	TIP should Deduplicate indicator input data when imported from multiple sources; Provide features to add context to and enrich threat intelligence-Ability to rank or assign severity of risk to intelligence and IOCs	
58.	Support Integrations with Security Products-Native support for STIX/TAXII integrations, Export threat intel data with secure API, Integrate with additional tools and information sources via RESTful API	

13. Detailed specification of Privileged Access Management PAM & PIM

Req ID	Specifications	Compliant (Yes / No / Partial)
A.		
1.	**The solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices.**	
2.	The solution should have a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc	
3.	The solution should be agentless i.e. does not require to install any agent on target devices	
4.	The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection	

5.	The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.	
6.	The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server.	
7.	The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism	
8.	The solution should also provide local authentication and all the security features as per best standards.	
9.	The solution should provide flexibility **user/device wise** for local authentication or enterprise authentication	
10.	The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors.	
11.	The solution should provide a method for creating new connectors with minimal intervention required from OEM.	
12.	The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.	
13.	The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment	
14.	The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacenter may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations	
B.		
15.	The solution shall perform password change options which is parameter driven	
16.	The solution should set password options every x days, months, years and compliance options via the use of a policy	
17.	The solution should be able to manage SSH Keys	
18.	For Linux/Unix servers, the solution should have an option to generate the SSH key pair directly from the tool.	
19.	Ability to create exception policies for selected systems, applications and devices	
20.	The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.	
21.	The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule.	

22.	Allow single baseline policy across all systems, applications and devices (eg one single update to enforce baseline policy	
23.	The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')	
24.	Ability to generate 'One-time' passwords as an optional workflow	
25.	Ability to send notifications via email or other delivery methods triggered by any type of activity	
26.	Ability to send notification via email to the user requesting the password that checkout is complete	
27.	All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.	
28.	The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities	
29.	The solution should have the ability to reconcile passwords manually, upon demand	
30.	The solution should automatically verify , notify and report all passwords which are not in sync with PIM	
31.	The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.	
32.	The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.	
33.	The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.	
34.	Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)	
35.	The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests	
36.	The solution should have the capability to seamlessly change the passwords for the large number of desktops. It should be able to handle floating Ips	
37.	The solution should have provision for secure offline access of managed credentials in case of vault failure (break glass scenario)	
38.	The solution should have provision to allow authorized users to upload their sensitive/confidential files in the Vault for secured and encrypted storage.	
39.	Files uploaded in Vault for secured and encrypted storage should be allowed to be shared between PAM users with an option to expire the share after defined period of time (in days).	
40.	Out of band electronic safes should be provided on every rotation and these should be available at will.	

41.	The solution should be able to automatically sync any out of sync passwords without using any external utilities (on target systems/applications)	
42.	The solution should also provide out-of-band vault capabilities (one or many)	
C.		
43.	The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user.	
44.	The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM	
45.	The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user.	
46.	The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+(client/), front-end database utilities on any combination of target account, group or target system and end-user.	
47.	The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc.	
48.	The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user.	
49.	The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.	
50.	The solution can restrict user-specific entitlements of administrators individually or by group or role.	
51.	The solution should have worklfow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc) and should be able to request for approval on the fly for those commands which are critical.	
52.	The solution can restrict target-account-specific entitlements of end users individually or by group or role.	
53.	The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired.	
54.	The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time.	
55.	System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH.	

56.	It should be possible to grant access to a managed asset using a specific method of access. For e.g. access to a SQL database ONLY through SQL Management Studio.	
D.		
57.	The solution should be able to support a session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments.	
58.	The solution should be able to **log commands** for all commands fired over SSH Session and for database access through ssh, sql+	
59.	The solution should be able to log/search text commands for all sessions of database even through the third party utilities	
60.	The solution should be able to log/search text commands for all sessions on RDP	
61.	The solutions should support selective option for enabling session based recording on any combination of target account, group or target system and end-user.	
62.	All logs created by the solution should be tamper proof and should have legal hold	
63.	The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group.	
64.	The tool can restrict access to different reports by administrator, group or role.	
65.	The tool generates reports in at least the following formats: HTML, CSV and PDF	
66.	System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts	
67.	The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats	
68.	The session recording should be SMART to help jump to the right session through the text logs	
69.	Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.	
70.	The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary	
71.	The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording. All other commands will be included.	
72.	The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution.	
73.	The proposed solution shall allow configuration at platform level to allow selective recording of specific device.	

74.	The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables).	
75.	The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.	
76.	The proposed system shall support full colour and resolution video recording.	
77.	The proposed system shall support video session compression with no impact on video quality.	
78.	The solution should provide an option to supervise privileged user activity with real time session shadowing capability.	
E.		
79.	The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.	
80.	The Solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance	
81.	All communication between system components, including components residing on the same server should be encrypted.	
82.	All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway)	
83.	The Administrator user cannot see the data (passwords) that are controlled by the solution.	
84.	Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).	
85.	The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.	
86.	The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)	
87.	The solution should not require direct third-party access to PAM Database	
88.	The solution should support common protocols to connect to PAM servers to ensure the best interoperability with environments.	
F.		
89.	The solution should have central administration web-based console for unified administration.	
90.	The tool uses Active Directory/LDAP as an identity store for administrators and end users.	
91.	The tool enables an administrator to define groups (or similar container objects) of administrators and end users.	
92.	The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one supergroup.	

93.	The tool enables an administrator to define a hierarchy of roles without limit.	
94.	Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.	
95.	Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly	
96.	The tool should have a provision to enable maker-checker configuration for critical administrative actions. For e.g. new user creation, on-demand password changes etc.	
97.	Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).	
98.	The solution should provide for self-service portal for users and devices for ease of on boarding both users and devices.	
99.	All administrative task should be done LOB wise i.e. Line of Business Wise	
100	All administrative tasks/actions should be logged along with change in configuration value i.e. value before change made and after the change made.	
101	The solution should have Auto-Onboarding Feature for both User and Devices without having to do any manual activity.	
G.		
102	The solution architecture should be highly scalable both vertically as well as horizontally.	
103	The proposed solution shall provide multi-tier architecture where the database and application level is separated.	
104	The solution should work at the network layer instead through a jump server. This will have achieve large number of sessions.	
105	The proposed solution shall provide scalability where it is not limited by the hardware. Also, the solution shall provide modular design for capacity planning and scalability metrics.	
106	The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.	
107	The proposed solution shall have built-in options for backup or integration with existing backup solutions	
108	The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.	
109	The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.	
110	The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.	
111	The proposed solution shall support both clients based (in the case where browser is not available) as well as browser-based administration	

112	The proposed solution should be 100% agentless that includes password storage, password management and session recording features.	
113	The solution must support parallel execution of password resets for multiple concurrent requests.	
114	The solution should provide fully failover from a single active instance to a backup/standby instance with a fully replicated repository	
115	The solution should support multiple active instances with load balancing and fully automatic failover to another active instance	
116	The solution if required should be available to install on a virtual sever	
117	The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. Please elaborate	
118	The solution should have an ability to have direct connection to target device as well as using secured gateway channel.	
119	The solution should have the capability to auto-onboard assets (VM's, databases, network devices, Public Cloud instance), groups, and discover accounts. It should be further able to configure rules to auto-assign the desired relationships/roles based on the least privileges.	
120	The solution does not require jump server architecture	
121	Solution should support hybrid architecture	
H.		
122	Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism.	
123	Ability to integrate with Bio-Metric Solutions	
124	Ability to integrate with Hard and Soft token solutions	
125	Ability to integrate with ticketing systems.	
126	Ability to integrate with Automation software's for enhancing productivity in the data center	
127	The proposed solution supports integration with the Hardware Security Module (HSM) devices to store the encryption keys.	
I.		
128	The solution can force the requestor of password / session to provide a reason, including a service desk incident ticket number, for the request.	
129	The solution can communicate with a workflow engine to verify an incident ticket number cited in the end user's request.	
130	The solution provides the capability to enable end users to retrieve (or reset) a target-system password only after approval by a designated approver (to allow dual control). Approval criteria can be based on any combination of target account, group or target system and end-user	

	identity, group or role, as well as contextual information such as day of the week or time of day.	
131	Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)	
132	Inbuilt ticketing system with multi level workflow approval with ticket level validation, risk and impact assessments as per group/tenant wise, Service type and user type. This ticketing system will help in creating a work order on an executor, who will then request access through the request workflow with this valid ticket	
133	Inbuilt ticketing system with 5 level workflow approval with ticket level validation, risk and impact assessments as per LOB wise, Service type and user type. This ticketing system to help in creating a work order on an executer, who will then request for the access through the request worklfow with this valid ticket	
J.		
134	The solution should be able to integrate with leading SIEM Solutions.	
135	The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords	
K.		
136	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.	
137	The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods	
138	Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.	
L.		
139	The solution should be able to perform auto discovery of privileged accounts on target systems and perform two-way reconciliation.	
140	The solution should provide feature for user governance on the target devices i.e autodetect users and schedule a governance workflow and user certification process with adequate review process.	
141	Map privileged and personal accounts on various target systems	
142	Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts)	
143	Ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key	
M.		

144	The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email	
145	The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email	
146	Customizable notification for command executed on SSH and Telnet based devices	
147	Customizable notification for command/Process executed on Windows	
148	Notification on target being access on criteria like Line of Business or Groups	
149	Solution should have threat analytics and customised reporting capabilities	
N.		
150	The solution should have inbuilt workflow to manage	
151	Electronic Approval based Password Retrieval	
152	Onetime access / Time Based / Permanent Access	
153	5 level approval workflows with E-mail and SMS notification with delegation rules	
154	Ability to provide for delegation at all levels in the workflow	
155	Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phone	
156	Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).	
157	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.	
158	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.	
O.		
159	Dashboard Capabilities should included real-time view of activities performed by the administrators	
160	The system shall have the ability to run all reports by frequency, on-demand and schedule.	
161	The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activities log	
162	The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records	
163	The solution should be able to report password lockouts (failure logon attempts)	
164	Ability to report password checkouts on systems and users requesting passwords	
165	Ability to report password lockouts (failure logon attempts)	

166	Ability to report on password change following verification process	
167	Ability to report on password status	
168	Reports should be customizable	
169	Audit data can be exported for use for any BI Tool	
170	Reports shall be automatically distributed by email	
171	Access to audit reports (and report configuration) shall be restricted to "auditor" end-users	
172	Ability to replay actual session recordings for forensic analysis	
173	The recorded session should be compressed and not take much space on storage and only active session has to be monitored	
174	The solutions should provide advanced analytics capability and provide risk score on all the sessions and tasks done by users.	
175	The solution must support session collaboration and delegation	
176	Dashboard - for at a glance critical events and password policies. *Describe your dashboard capabilities*	
P.	**Threat Analytics**	
177	The solution should have threat analytics and customized reporting capabilities	
178	The PAM solution supports creation of custom reports.	
179	The PAM solution has automated report query capability.	
Q.	**Privileged Elevation & Delegation Management**	
180	Solution should offer agent-based privileged elevation and delegation management.	
181	The solution should offer agent-based privileged elevation and delegation management for Linux/Unix Systems.	
182	Session recording should be available for PEDM scenarios on Windows systems	
183	Session recording should be available for PEDM scenarios on Linux/Unix systems?	
184	Describe any security mechanisms that are available, for example, the ability to prevent/control shell escapes and the ability to prevent/control spawning subprocesses.	
185	The solution should be able to elevate privileges in Windows environment for remote execution scenarios	
186	The solution should be able to elevate privileges in Linux/Unix environment for remote execution scenarios	
R.		
187	OEM Should have 24*7 support center in India (Please share Support center details & address)	
188	The PAM solution should be covered by the Gartner Magic Quadrant for last three consecutive years (2021, 2022 and 2023) & should be in Leaders/Challengers quadrant. (MQ Gartner report to be submitted)	
189	The PAM Solution must be a leading, mature, internationally recognised and widely used brand that has been in existence for at least 10 years. (Please provide certificate of incorporation)	

190	The offered PAM OEM Solution must be certified for Common Criteria Certificate EAL 2+ and supporting certificate document should be submitted during bid submission	
191	The PAM solution should be successfully deployed and running for the last 3 years in India in minimum 5 PSUs/Private Bank/Government/Listed Entities in India with relevant scope of implementation with current usage of 1000+ Users and 3000+ devices (PO/Work order copies to be submitted for the same)	
192	The proposed OEM should have average annual turnover of Rs. 50 Crs during the last three financial years	
193	(Only Company's / Firm's figures need to be mentioned from its operations in India. (Not to include subsidiary, consortium, affiliate or group entities figures)	
194	The offered PAM OEM should should have SOC II type II certification	
S.		
195	Does the solution require an agent installed on the endpoint?	
196	Can the agent be installed via the following methods:	
	-SCCM \ Intune	
	-GPO	
	-Other	
	-CLI	
197	Can the solution be deployed to the following endpoints:	
	-Windows 10 Pro	
	-Windows Server 2012 R2 and above	
	RHEL, Ubuntu, CentOS, Oracle Linux , etc	
	MacOS	
198	Does the solution allow scripting toolkits to install software without impacting them:	
199	Does the solution override the local admin groups of the endpoint? Or admin groups pushed by GPO?	
200	Does the solution prevent removal of the agent? If so how?	
201	Describe the agent behavior if an endpoint is offline/unable to contact the administrative tool.	
202	Describe the agent removal process	
203	Does the solution have the ability to create profiles based on:	
	-Device grouping	
	-User account grouping	
	-AD Org unit	
	-Endpoint OS	
T.		
204	Ability to Whitelist\Blacklist application installation by:	
	-Software publisher	
	-Application	
	-Software category/genre (Application Categorization)	

	-File hash	
205	Ability to Whitelist\Blacklist application execution by:	
	-Software publisher	
	-Destination location? By file, directory, recursive structure	
	-Application	
	-Software category/genre (Application Categorization)	
	-File hash	
206	Allow time-based user account elevation (ie. elevate credentials for a period of time)	
207	Allow end user to request account elevation, please explain process in details section	
208	Universal admin privilege groups (ie all fields techs are admins on a group of machines)	
209	Ability for technician \remote support to remote in with elevated privileges?	
210	Ability to elevate script files like batch, powershell, python, etc	
211	Ability to restrict USB mass storage access	
212	Ability to restrict bluetooth file sharing	
213	Ability to record sessions in text and video logs	
214	Ability to track geo location of the device	
U.		
215	Auditing & Event Logging of:	
216	-Access elevation events	
217	"Read only" reporting to audit what activities endpoints require local admin permission	
218	Reporting of systems with accounts as local administrator	
V.		
219	Ability to enforce Azure Active Directory Single-Sign-On integration	
220	Role based access to console (ie technicians manage a subset of devices, read only access, etc.)	
221	Ability to support SAML authentication	
W.		
222	Ability to detect anomalous user behaviour	
223	Ability to train and suggest policies based on user behaviour	

14. Detailed Specifications of Network Management System (NMS)

S.no	Specifications

A.	EMS
1.	The proposed EMS solution shall provide at a minimum the following functions: a. Fault & Performance Management b. Auto-discovery of Nodes for the monitoring c. Event Management & Log Management d. Server, Storage and other Infrastructure Management e. SLA Management & Monitoring f. Capacity planning and Management By Using AI/ML techniques g. The solution should have unified dashboard for single pane of glass of view h. The proposed solution should support high availability. i. The proposed solution should be supplied with minimum license, and scalable to handle the future growth without any change in architecture.
2.	All the required hardware and software will be in bidder's scope.
3.	"All required modules or solutions, including NMS, ITSM, Asset Management, SSO, and Patch Management, must be provided by the same OEM. Solutions from third-party providers, white-labelled products, co-branded offerings, or resellers will not be accepted
4.	The proposed EMS/NMS solution MUST have at least 13+ deployments in Indian Governments/Smart city safe city/ BFSI. Necessary documents like PO and Minimum 3 sign off/completion certificate would be required need to submitted during the bid time.
5.	The proposed solution should have deployment reference where solution is able to monitor the 50K LAN devices in single project. Supporting document like PO/WO Copy should be submitted during the bid submission time.
6.	The proposed Solution NMS, ITSM, Log management solution should be trusted from Trusted Telecom Portal. Necessary Proof details should be submitted during the bid time.
7.	It should be secured with single sign-on (SSO) and must have authentication through LDAP. EMS, SSO engine & directory services solution should be from the Same OEM.
8.	The proposed solution shall facilitate the analysis and display of status information from all the type of devices attached to the system by using various polling techniques like ICMP, SNMP(v1,v2c,v3) etc.
9.	The proposed solution shall provide the ability to view the network topology and its associated IP SNMP/ICMP enabled devices including switches and other IP devices connected over the network.
10.	The proposed solution should be able to do performance monitoring of each connected device on various listed KPIs like: 1. CPU utilization 2. RAM utilization 3. Memory utilization 3. Bandwidth utilization 4. Disk Space utilization 5. Error packet loss 6. TCP Segments 7. UDP Segments 8. Packets IN/OUT 9. IN/OUT Traffic Utilization
11.	The proposed solution should support threshold-based monitoring in case of set threshold breach (like Bandwidth, CPU, Memory, Disk Space etc.) and critical alarm should be generated with severity RED color demarcation and triggering the same via email, SMS etc.

12.	The proposed solution should include all hardware and software required to configure, control and monitor the network connected SNMP/ICMP based devices
13.	The proposed solution shall provide discovery & inventory of physical network devices and other IP devices
14.	The proposed solution shall be able to monitor the utilization of physical as well as virtual server
15.	Solution should support API integration with third party application
16.	Solution should cover all the aspects of FCAPS
17.	Solution should support cloud and Virtualisation from day one
18.	Solution should have predictive analysis from day one
19.	All the required module of EMS should be from same OEM
20.	NMS shall support client–server-based architecture. Client being GUI/web browser-based access with secure interface to the server
21.	The EMS should support provision of creation, addition, deletion, updating and viewing capability of the managed network
22.	The proposed solution shall be capable of managing/monitoring any SNMP/ICMP device from any vendor/providers.
23.	Solution should have business service monitoring capability
24.	Solution should have role & privileges-based access from day one
25.	Solution should support LDAP integration from day one
26.	The solution should support SSO from day one
27.	The proposed solution must be an industry standard solution from an OEM that is minimum CMMi LEVEL 3. Certification copy for the same to be submitted along with bid.
28.	The proposed solution must be an industry standard solution from an OEM that is ISO 27001:2013 & ISO 9001:2015, ISO: 45001:2018, ISO 15408-1:2022, ISO/IEC 20000, ISO 14001:2015 & ISO 27034 to ensure the quality and security Certification copy for the same to be submitted along with bid.
29.	The solution should have flexibility to customize the dashboard and reports as per the customer requirement. Detailed engineering will do during the implementation phase.
30.	The proposed solution should have the unified view/single pane of glass dashboard view
31.	The dashboard should have the business-critical monitoring section where maximum three node/device can be displayed with fault and performance data.
32.	The proposed solution should have URL monitoring capability
33.	Following parameter need to consider for the URL monitoring i.e. Response time in MS, SSL expiry time, url (up/down) status.
34.	The proposed tool should be able to monitor various KPI like CPU utilization, Load average, RAM & Hard disk.
35.	The proposed tool should be able to monitor various options to visualize the data like Line chart, Table, Pie chart.
36.	The proposed tool should be able to monitor vms as well.
37.	The proposed solution should have the ability to do the configuration backup and restore functionality.
38.	The proposed solution should have the inbuilt troubleshooting tools includes, ping, nslookup, traceroute.

39.	The proposed solution shall have intelligent discovery process i.e. identify devices within a specified IP range, categorizing them into network devices and servers, along with detailed vendor and model information.
40.	The proposed solution should support Layer 2 and Layer 3 topology discovery automatically using various protocols. Topology should be auto generated based on neighbour ship with other devices. However, topology should be editable as per Employer/Customer requirements.
41.	The solution should have Integrated Web based feature to build Network topology. No separate client window to configure network topology. Hovering over a device or link in the topology view should display key statistics such as IP address, hostname, up/down status, traffic details etc.
42.	The proposed solution shall provide many different types of topology representation to perform the following: 1. Display physical connections of the different devices being monitored in the system and display flat maps of the entire network or networks in a single view 2. Display maps based on geo locations
43.	The proposed solution shall support SNMP v3 (or the latest version) with OID values of multiple vendor/OEM, ICMP, RestAPI, SSH, WMI, HTTPS, HTTP & TELNET protocols
44.	System should have node/interface tagging and filtering options as defined below: i. based on device type ii. based on customer iii. based on location
45.	The proposed solution shall support a minimum polling interval of 60 Seconds, with the option to customize the interval as needed.
46.	The proposed solution shall support provision to change the polling interval to any frequency depending on the priority of the individual node/device
47.	The proposed solution shall have the provision to disable and enable the polling of specific type of node/devices
48.	The proposed solution shall have the following capability with respect to event management: Solution should generate event for all the monitoring devices. Solution should generate events on regular Polling interval Solution should be able to classify and assign different levels of severity to events.
49.	The proposed solution shall provide Event Filtering, Event De-duplication, Event Suppression and Correlation capability to let user focus on the critical event that affects the operations.
50.	The proposed solution shall detect & highlight Faults & outages related to service (abnormal situations) in near real-time.
51.	The Proposed solution shall support alert/alarm acknowledgement and resolution capabilities (tagged with username)
52.	The proposed solution shall support global threshold and it should have option to define individual node/group of nodes/interface/group of interface statistics level threshold.
53.	The solution shall support: - Define and store resource utilisation thresholds for individual nodes or interfaces - Support comparison of actual availability/performance with agreed levels - Alert if any breach of threshold value - Alert should be go on SMS/EMAIL and it should also capture as critical event in dashboard.

	54.	The solution should be able to retrieve and display fault, performance (including but not limited to packet loss, jitter, latency, throughput, CPU utilization, memory utilization etc.), inventory, software/firmware versions and SLA data in a same/single view/window. It should also offer options to export these views/data in various formats such as PDF, Word, Excel, HTML etc. Additionally, the system should support the addition of custom fields to include any extra information about the nodes/devices.
	55.	The proposed solution shall monitor all traffic from all the interfaces of the network device. Solution shall provide traffic utilization based on individual interface level, nodes level or based on the group by location, etc. as an Avg, Min and Max Bandwidth utilization/throughput or any custom monitoring parameters.
	56.	The proposed solution shall be able to display of multiple parameters such as latency, jitter, throughput, packet loss, CPU, Memory etc. for a node wise in single Widget
	57.	**The SLA calculation / Isolation report should consider both the Primary and Secondary links together, rather than individually. Downtime will be measured when both links are down for internal / customer reporting,** SLA Calculation module shall inbuilt from Day1.
	58.	The proposed solution should have capability to configure the maintenance period for any node. When node is in maintenance period there is no polling done and the SLA clock on the node is stopped.
	59.	The proposed solution should have following Reports & Dashboard functionality: - Should have pre-defined Availability, Performance , Capacity Dashboards - Solution should have option to drag and drop dashboard configuration in custom dashboard - Should have option to add multiple type of widgets along with (Tabular, Summary, Multiple Graph in custom dashboard). - Should have option to select various widgets such as recent events, host statistics, host problems Filter, Sort, Search, Group by,-Event Type - Export option to PDF , XLS etc.
	60.	The proposed solution should be able to automatically generate daily reports that provide a summary of the all monitored nodes as well as custom Reports and that are automatically sent by email at a pre-defined schedule to any recipient or save into any specific folder or drive.
	61.	Solution shall support Real-Time (Acceptable delay up to 65 seconds) report generation on links up/down status and other downtimes for a given past duration
	62.	The proposed solution provides standard reports that display current status of nodes and interfaces. Reports could be viewed on daily graph (5-minute average), weekly graph (30-minute average), monthly graph (1 hour average) and yearly graph (1 day average)
	63.	The proposed solution should be able to extend end customer dashboard (Self-care portal) will have at least following information: 1. Display real-time (Acceptable delay up to 65 seconds) performance data such as Uptime availability, Bandwidth utilization, latency, packet loss, etc. 2. Access to historical performance data for trend analysis. 3. Visual indicators for network health and performance status. 4. The network availability graph & reports shall be generated from the end customer dashboard

64.	The proposed solution should support Role based access control (RBAC). i.e. Dashboard should be able to create multiple separate profiles (of different customers) that monitors and displays specific nodes belonging to those customers only.
65.	The proposed solution should support different level of authorization for users such as view only, specific rights, administrators etc.
66.	Solution shall support for sending alert via E-mail & SMS Necessary integration is in the scope of the Bidder. Providing respective Gateways are in the scope of Employer.
67.	The proposed solution shall provide a notification mechanism that allows administrator to define what notification channel such as Email/SMS etc. to be used in different time of days, and able to trigger multiple notifications to alert multiple person and actions
68.	The proposed solution shall support instant diagnosis of the node status through Ping, WMI, Telnet, SNMPwalk, Traceroute, Nmap
69.	Raw data shall be retained for a period of 12 months and post this period, data shall be aggerated into hourly format for another 12 months
70.	The proposed solution shall provide alert console with alert summary such as no. of network alert, server alert, virtualization alert, cloud alert, application alert etc.
71.	The system shall have provision to overlay alert on reported metric to understand alert triggering behaviour across multiple drill down pages
72.	The proposed solution shall provide default event dashboard to identify, accept and assign generated alarms
73.	The NMS shall allow mass programmable equipment configuration by the mean of scripts.
74.	The NMS shall allow infrastructure-wide software image update for baseline version management
75.	The proposed solution should be able to take back up of running and startup configuration of network devices. It should also provide versioning for backup to track changes.
76.	The NMS shall offer a unified user interface for wired, wireless network and Server Infra.
77.	The solution should allow the admin to easily provision, manage and maintain a network infrastructure with alarms
78.	The solution should provide full visibility into wireless, devices and Servers.
79.	The management solution should act as comprehensive tools for Network/Device configuration (for switches), monitoring, alert monitoring and management.
80.	It should be web-based interface with customizable dashboard
81.	Monitor network bandwidth on each interface and shall able to set policies/alerts at each interface without any additional license's implication.
82.	The proposed helpdesk system shall be minimum ITIL V3 pink verify certified on six processes I.e. Incident Management, Problem Management, Request Management, Change management, Service level Management & Service Asset & Configuration Management.
83.	Tool should have automatically create a distinct and unique identifier and number for each incident Record
84.	Solution should have Simple/Routine Issues: Need a simplified ticket opening method for simple issues.

85.	Solution should have Must allow free-form description of problem: Must request detailed information from end user.
86.	Solution Must provide categories for user to select.
87.	Must automatically capture and attach screenshot i.e. OCR to incident creation feature
88.	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other tools/solutions
89.	Must be automatic based on category chosen by end-user and technician skill set.
90.	Manual reassignment must be possible, by any technician or manager.
91.	All details of ticket entered by end user must be viewable by technician within application.
92.	Technician must be able to edit any information in ticket to correct assumptions or incorrect information given by end user.
93.	E-Mail: System must allow direct e-mail communication between technician and end-user, and log all e-mail contact in the ticket.
94.	Solution should have GUI based configuration for the email to incident features
95.	Attachment of the email should be stored in the helpdesk portal with the time stamp and reference email Id for audit purpose
96.	Any further communication on the email should be captured in the helpdesk portal as a public log for the complete end to end tracking of the incident.
97.	The solution should have GUI based configuration for the notification of all the stakeholders as required
98.	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming
99.	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.
100.	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
101.	The proposed helpdesk system shall integrate tightly with the knowledge tools and CMDB and shall be accessible from the same login window.
102.	The solution should have the mechanism to define and measure the FMS performance like TTO (Time to Own), TTR (Time to resolve) or equivalent parameters for the incidents and request in the Service Desk Portal
103.	It shall allow IT team to create solution & make them available on the end – user login window for the most common requests.
104.	The proposed solution should have problem Management & Change Management.
105.	The proposed helpdesk solution should have the IVRS capability for the better interoperability IVRS/Contact center and ITSM solution should come from the same OEM and it should be Pre integrated. The OEM should share the atleast 2 reference where the EMS and IVRS/contact solution supplied in same project. Documentary proof must be submitted during the bid time.
106.	The proposed solution should have AI enabled Chabot to help the resolution of tickets by finding the relevant sections across the knowledge materials.
107.	The proposed solution must provide comprehensive software and hardware asset lifecycle management solution including requisition, procurement, inventory, deployment, and contract management.
108.	The proposed Solution should support Auto discovery of assets by using SNMP protocols.

109.	The proposed should track and control all hardware assets installations, moves, additions and changes (IMAC). It should provide deep visibility into assets owned, where they are located, maintenance details, compliance etc.
110.	The proposed solution should provide inventory of hardware and software applications on Servers / desktops including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them.
111.	The proposed solution should provide reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs
112.	The proposed solution should have the web-based dashboard, the dashboard solution should support on fly customization of dashboard view without any code change. Also, it should not impact on application.
113.	The proposed solution should support Role based access control
114.	The proposed solution should store detail asset information on hardware and software inventory
115.	Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops
116.	Ability to provide unified Asset, Change and Configuration management, with automated updates of related assets and CI data. It should include: -
117.	a. Automatically link an asset to CI or vice versa
118.	b. Automatically update an asset when CI gets updated and vice versa
119.	The proposed solution should be able to track changes by maintaining history of an asset
120.	The proposed solution should provide the facility to support event policies such that predefined actions can be triggered, such as sending an email notification, when key events occur such as software license violations, AMC expiry etc.
121.	The proposed solution should have the ability to offer remote control capabilities for Windows environment
122.	The proposed solution should have the ability to support multiple connection protocols for remote control, including RDP, VNC etc.
123.	The proposed solution should support remote reboot capabilities of the endpoints
124.	Ability to provide secure communication between the server and agent
125.	Ability to allow multiple remote management sessions to be opened concurrently with easy switching between the sessions
126.	Asset Management tool should be able to give the patch management capability inherently built in the system, so to apply the relevant patches from the asset itself. This should be available from day zero, with tightly couple architecture, such that application works smoothly. external integration should not be done
127.	Solution should have the barcode-based asset tracking and management
128.	Asset Management tool should have option to maintained the asset financial data
129.	The proposed asset management tool should have barcode generation and barcode reader functionality.
130.	The proposed asset management tool should have the Mobile APP for the barcode scanning.
131.	The proposed asset management tools should be able to do the live tracking of the asset.
132.	The proposed solution should have the agent for the OS (Windows/Linux) based agent

133.	The proposed solution should be secured with single sign-on (SSO) and must have authentication through directory services. For enhanced security and effectiveness Asset Management, SSO engine & LDAP/directory solution should be from the same OEM.
134.	The proposed Solution should support centralized CMDB
135.	The proposed solution should have on fly customizable dashboard option.
136.	The Proposed solution should have the following functionality: 1. Asset details 2.Asset Service 3. Risk Analysis 4. Policy Impact
137.	The proposed solution provide Safeguards associated, inventory information (all info, like IP, MAC, Size, temp, etc.)
138.	The proposed solution should have the single Dashboard view of Asset and Risk associated with that by selecting the asset everything should be tracked/visible for assets
139.	The proposed solution should be integrated with the ticketing platform, so automatically every incident and impacted asset should be seen, with all details.
140.	The proposed solution should have risk analysis dashboard
141.	The proposed solution should have the capability to define the owner and custodian, if there are many tickets on an asset, the custodian may be mishandling and should be changed.
142.	The proposed solution should have option of bulk upload option for the on boarding of assets
143.	The proposed solution should have inbuilt barcode generation and mobile based barcode scanner.
144.	The proposed solution should support bulk barcode generation capability.
145.	All the required module i.e. Asset Management, Patch Management, Remote access software should be from same OEM and Pre integrated from day one.
146.	The proposed solution should have deployed in various got organizations, provide at least 3 references. Necessary documents like PO/WO copy should be submitted during the bidding time.
147.	The proposed solution should have deployment reference where solution is able to manage the 50k assets in single project. Supporting document like PO/WO Copy should be submitted during the bid submission time.
148.	Shall be a multi-platform application / system with support for Windows (Desktop, Server) and Linux (Ubuntu, Debian, Centos, Red hat)
149.	Automatically scans the endpoints to find the missing security patches at OS level as well
150.	The proposed solution should be supplied with minimum 30 endpoints license.
151.	Solution should have functionality to downloads the required patches for deployment
152.	Shall support Customized Deployment Window/ scheduling of patches for the deployment
153.	Shall support to download and keep the patches in client machine before the deployment window, so that deployment window can be used effectively.
154.	Automatically installs the missing patches to endpoints as per the configured task
155.	Shall support Customized Reboot Policy

156.	Shall support all types of Microsoft updates which includes Feature Pack, Cumulative, Rollup, Preview, Optional, etc.
157.	Shall support Security Updates for different Linux Flavours (Ubuntu, Debian, Centos, Pardus, Redhat and SUSE)
158.	Shall support patch management of major Third-Party application for Windows, MAC and Linux
159.	Shall support various predefined reports with extensive filter options
160.	Shall support scheduling the reports to multiple mail address
161.	Shall support creating custom report with available data
162.	System shall support configuration for calculating the client health based on different parameter like Severity, Patch Approval,
163.	Shall support to automate the patch testing process in your test environment
164.	Shall support to automatically approves the patches based on the patch deployment status in test machines
165.	Shall support creation of machines group for better management
166.	Shall support creation of dynamic group based on different parameters like System Type, Operating System, etc.
167.	Shall support cleanup of the Patch Store regularly for managing the disk space
168.	Shall support Failover server for zero downtime of Server. The server shall be installed in HA mode in DR
169.	All the hardware, software and licenses required to run the system shall be part of the bid and will be in bidder scope.
170.	Shall support setting up of jump server to create an air-gapped environment for downloading the patched required to be installed in the network
171.	Shall provide API's to export data to different tools as required and also to perform various actions like integration with other systems
172.	Define Role based User Administration
173.	Supports SAML Authentication
174.	Supports two/multi factor authentication, from same OEM, to make sure the integrity, Tool should be securely accessed, with capability inherently built in the system, so to have secured access as a legacy capability. This should be available from day zero, with tightly couple architecture, such that application works smoothly. external integration should not be done
175.	Patch management solution should have the at least 5 deployment reference across various govt. organizations, covering around 5000 endpoint, necessary documents like PO/WO copy should be submitted during the bid time.
176.	The proposed solution shall support Flow monitoring and traffic analysis for Net Flow, J-Flow, sFlow,IPFIX technologies.
177.	The proposed solution shall supply with minimum 1 GBPS.
178.	The proposed solution shall provide a central web-based integration point across any of the flow protocols and shall be able to report from a single console.
179.	The proposed solution shall be of passive type and should not cause any performance overheads.
180.	The proposed solution should be able to show real-time network traffic and active hosts
181.	The proposed solution should be able to produce long-term reports for several network metrics including throughput and L7 application protocols
182.	The proposed solution should able to display the top talkers (senders/receivers), top ASs, top L7 application protocols

183.	The proposed solution should be able to monitor and report live throughput, network and application latencies, Round Trip Time (RTT), TCP statistics (retransmissions, out of order packets, packet lost), and bytes and packets transmitted
184.	Solution should be able Geolocation and overlay hosts in a geographical map
185.	The proposed solution should be able to analyse IP traffic and sort it according to the source/destination
186.	The proposed solution should support for IPv4 and IPv6
187.	The proposed solution should be able to Layer-2 support (including ARP statistics)
188.	Syslog server is a logging server that allows for the centralized collection of syslog messages, known as events, from a variety of networking devices such as routers, switches, and firewalls, in addition to servers running a variety of operating systems.
189.	The Solution can be hardware/virtual appliance. Sizing and infra for virtual solution shall be in the bidder's scope.
190.	The proposed solution should come with minimum 5 gb/day consumption rate.
191.	The proposed solution should be deployed in HA.
192.	Syslog is a powerful platform that allows for easy log management of both application and devices.
193.	Syslog server receives data from its clients installed on different servers ,and a web interface, which visualizes the data and allows to work with logs aggregated by the main server.
194.	**Proposed solution should support following methods to collect the log:** • Collecting Data • Syslog (TCP, UDP, AMQP, Kafka) • GELF(TCP, UDP, AMQP, Kafka, HTTP) • AWS - AWS Logs, FlowLogs, CloudTrail • Beats/Logstash • CEF (TCP, UDP, AMQP, Kafka) • JSON Path from HTTP API • Netflow (UDP) • Plain/Raw Text (TCP, UDP, AMQP, Kafka) • Sidecar
195.	**Dashboard** Combine widgets to build fully customized, predefined data displays so everything important is just one click away. Drill-down to explore your data further. • Per device dashboard • Per server dashboard • Group Application dashboard
196.	**Audit Analysis** • Analytics dashboard • Periodic reports • Customized reports • Anomaly detection
197.	**User Management** • Multiple account types • Role based Access Control • Use Groups

	198.	**Servers** • Windows • Debian • Suse • CentOS • RedHat • Unix • Linux • Solaris • Ubuntu
	199.	**Solution should support various Device Types for consuming the syslog:** • Server • Routers • Switches • Firewall • Access Controller • Load Balancer • Access Point • UPS • SIEM • DDOS • IPAM • Wired Devices • Wireless Devices
	200.	The proposed solution should support to write the connectors/parsers in case of by default is not there.
	201.	The proposed solution should give the alert in case of any device is not sending the logs
	202.	The proposed solution should support the RBAC.
	203.	Solution should support alert integration to 3rd party system via API
	204.	Solution is able to search all historical logs without the need to reingest or rehydrate from an alternate location
	205.	The proposed OEM should be present in India from last 9+ years. Documentary proof must be submitted during the bid time.
B.		**AI/ML Based Predictive Analysis**
	206.	Predictive Analysis: Solution should have Predictions based on Historical Data, of various performance KPI using AI/ML algorithms.
	207.	Solution should be able to do the capacity planning by using AI/ML algorithms
	208.	Predictive analysis allows for proactive problem-solving by forecasting potential network issues
	209.	The proposed AI/ML models can analyze historical data to predict peak usage times and network congestion
	210.	Predictive analysis can identify patterns indicative of security threats or abnormal behavior, helping to detect and mitigate cybersecurity attacks as well.
	211.	By analyzing historical data and predicting future network loads, AI/ML models should be able to assist in capacity planning, which will ensure the Network administrators can scale resources appropriately, ensuring that the network can handle increasing demand without performance degradation
	212.	AI/ML-based predictive analysis provides valuable insights based on data patterns. This allows network administrators to make informed decisions, optimize network performance, and align infrastructure investments with actual usage patterns

C.	**AI/ML Based prescriptive Analysis**
213.	The proposed solution will help to tell the course of action needs to take on the basis of predictive data
214.	Prescriptive analysis enables the NMS to dynamically adapt to changing network conditions. Machine learning models can learn from real time data, adjusting recommendations and actions based on the current state of the network.
215.	By leveraging machine learning, prescriptive analysis can help reduce false positives in network monitoring alerts.
216.	AI/ML models can provide tailored recommendations based on the specific characteristics and requirements of a given network. This customization ensures that the prescribed actions align with the unique features and demands of the network environment
217.	Prescriptive analysis can contribute to the identification of potential security threats and vulnerabilities. By analyzing network behavior patterns, the system can recommend security measures and responses to mitigate risks and protect against threats.
218.	AI/ML-based prescriptive analysis enables the automation of routine network management tasks. This reduces the workload on network administrators and allows them to focus on more strategic and complex issues.
219.	By providing actionable insights and recommendations, prescriptive analysis aids network administrators in making informed decisions.
220.	The proposed solution should ensure that the prescriptive analysis capabilities of the NMS remain up-to-date and effective over time.
D.	**AI/ML Based descriptive analysis**
221.	The proposed solution should have data statistically to tell what happened in the past in forms of graphs, charts, reports, and dashboards
222.	Descriptive analysis powered by AI/ML can automate routine tasks like log analysis, performance monitoring, and incident detection
223.	By automating repetitive tasks and optimizing resource allocation, AI/ML-based descriptive analysis contributes to cost efficiency in network management
224.	By proactively identifying and addressing potential issues, AI/ML-based descriptive analysis helps reduce network downtime.
225.	Descriptive analysis can generate personalized insights for different users or departments within an organization. This tailoring of information ensures that relevant network data is presented to specific stakeholders, facilitating better decision-making.
E.	**Anomaly detection**
226.	AI/ML can be used to create models that understand Service Behavior
227.	Any deviation from the norm can trigger alerts, helping in the early detection of anomalies and potential problems
228.	Anomalies can be from Users or Entities.
229.	Solution provides risk profile and scoring of the user/entities based on behavior tracts
230.	Anomaly detection algorithms can identify deviations from normal network behavior, allowing for the early detection of potential issues.
231.	AI/ML-based anomaly detection helps in pinpointing these irregularities like unauthorized user access, contributing to the identification and mitigation of security threats.
232.	AI/ML models can learn normal patterns and adapt to changes, reducing the number of false alarms and improving the accuracy of anomaly detection.

233.	Anomaly detection models can adapt to changes in network behavior over time. This adaptability is essential in dynamic network environments where normal patterns may evolve.
234.	Anomalies related to network performance, such as unusual spikes in traffic or latency issues, can be indicative of underlying problems.
235.	By identifying anomalies related to resource utilization, AI/ML models assist in capacity planning.
236.	Machine learning models can perform behavioural analysis on network users and devices. By understanding normal behavior, anomalies such as unauthorized access or suspicious activities can be identified, enhancing overall network security.
237.	Anomaly detection provides a faster response to incidents by promptly alerting administrators to abnormal activities
238.	Anomaly detection systems continuously monitor network data in real-time, providing a proactive approach to network management.
239.	Anomaly detection model should contain multifaceted, encompassing early issue detection, security threat identification, adaptability to changing network conditions, and improved incident response.
F.	**Risk Analysis and Policy Impact**
240.	The proposed solution should have AI/ML based Risk Profiling & Scoring of asset
241.	Asset is tracked/mapped against compliance/Policies
242.	All policy violations are flagged for risk analysis
243.	Policy impact of each violation is shown
244.	Develop risk mitigation strategies to safeguard critical assets and sensitive information.
245.	The proposed solution should be able to classify assets based on their sensitivity and importance etc.
246.	Implement robust access controls to ensure that only authorized personnel have access to sensitive asset management information
247.	Assess and manage the security risks associated with third-party vendors involved in asset management services.
G.	**AI Powered Service Desk solution**
248.	Solution should be leverage with Smart Ticket Creation & closer
249.	Solution should have OCR to ticket creation option
250.	Solution should have Intelligent Routing mechanism by using workflow automation
251.	Solution should have AI/ML based Analytics dashboard for Decision-Making
252.	Solution should have Intelligent notification mechanism for notifying the incidents to the assigned engineer.
253.	ML models can learn normal network behavior and raise the tickets when deviations occur.
254.	Machine learning models can predict potential incidents by analyzing historical data and identifying trends or patterns that may lead to issues.
255.	ML algorithms can prioritize incidents based on their severity, impact on business operations, and potential risks. This helps incident response teams focus on critical issues first, improving overall response efficiency.
256.	AI-driven automation can execute predefined incident response actions based on the type and severity of the incident to facilitate quicker understanding of incident details and accelerates decision-making processes.

257.	ML algorithm to analyze historical incident data to identify recurring patterns and trends for implementing preventive measures and improving overall security posture.
258.	Service desk solution has GEN AI-guided step-by-step troubleshooting for common issues.
259.	The proposed solution should have enhanced knowledge base (KB) search capabilities, making information retrieval more accurate, efficient, and user-friendly

15. Detailed specifications of Endpoint DLP

End Point DLP
Proposed solution should on prime.
Proposed Solution should be able to identify Sensitive Data using Sensitive Keyword based markers, Pattern/Regex based markers, Unstructured Fingerprinted Data based markers, file attributes-based markers
Proposed Solution should be able to block data transfer via devices (USB drives, MTP, Printers, CD/DVD, Bluetooth Connected devices etc) and prevent Data Loss via devices (USB drives, Printers) using content identification
Proposed Solution should be able to prevent Data Loss via restricted enforced encryption of USB storage devices and identify and whitelist USB storage devices for internal use
Proposed Solution should be able to Block Web File Uploads based on Whitelisted or Blacklisted Domains or Email Addresses (Sender domain), File Type, File Attributes (Password Protection / Data Classification Meta Tags) and File Names while also sensitive content inside files
Proposed Solution should be able to generate alert for Web Uploads based on inspection and identification of sensitive content inside HTTP POST/PUT content in browsers
Proposed Solution should be able to Monitor, Log and Block all Application Network Activity
Once deployed Proposed Solution should be able to Scan, Inventories, Categorise and List all applications running in the organisation environment (including all running versions) for identification of any rogue applications
Proposed solution should be able to block all rogue applications from making a network connection by way of an essential application whitelisting method
Proposed solution should be able to Sandbox applications; to restrict them from only making network connections to specified destination IPs or URLs
Proposed solution should be able to Bypass specified applications (eg; Core systems etc), to ensure no interception, logging or blocking of safe and recognised outbound traffic
Proposed solution should be able to Bypass Logs and Shadow Logs; based on email/web domains/Ips
Proposed Solution should be able to Monitor, Log and Block all Browser/URL Activities
Proposed Solution should support pre-defined and categorised Web/URL list as per industry standards
Proposed Solution should support Additions, Changes, Removals or Customisation of Web Categorisation Lists
Proposed System Should Support creation of Custom Web Categorisation Lists
Proposed Solution Should enable blocking or allowing of Web/URLs/IPs based on Whitelisting or Blacklisting approaches
Proposed Solution should have the ability to inspect content using Optical Character Recognition (OCR) for standard and clear images no less than 72 DPI and rotation not greater than 3 degrees.
Proposed Solution should have the ability to identify User malicious activities across avenues of Data Theft, Productivity Loss, IT Misuse, Financial Loss, Operational Loss, Inappropriate Employee Behaviour and Cyber Security Risks.
Proposed Solution should have the ability to identify User malicious activities and behavioural anomalies across channels of Application Activity, Application File Access Activity, Browser Activity, User Activity Time Tracking, CD/DVD Activity, Data At Rest Activity, File Upload Activity (Web and FTP), Gmail and OWA activity, Outbound Network file transfers, Printer Activity, Web Search Activity, SMTP based Outbound Email Activity,USB activity
Proposed Solution should have a highly customisable Incident rule creation interface; with the ability to add multiple parameters of triggers behind each incident for minimising false positives
Proposed Solution should be capable of Shadow Logging Emails, File Uploads, USB Transfers, Print, Application File Access, Web Uploads etc

Proposed Solution should be able to handle if different users were to login to same device in tandem or vice versa; trailing user activity across devices and device activity across users and reporting them in accumulation by importing and mapping through Active Directory Users
Proposed Solution should be capable of logging all User/Device activity for Application Activity, Application File Access Activity, Browser Activity, File Upload Activity, FTP File Upload Activity, Gmail Web Activity, Network File Share Activity, Outlook Web Activity, Search Engine Activity, SMTP Email Activity, USB, Printer Activity, Data-at-Rest Activity
Proposed Solution should be capable of Entity Level Behaviour Analytics depiction of Application Activity, Application File Access Activity, Browser Activity, File Upload Activity, FTP File Upload Activity, Gmail Web Activity, Network File Share Activity, Outlook Web Activity, Search Engine Activity, SMTP Email Activity, USB, Printer Activity, Data-at-Rest Activity
Proposed solution should be able to initiate event-triggered screenshot for sensitive application activity and sensitive window title-based activity forensic evidence
Proposed Solution should present flexible deployment options for On-Premise Server with support for DC and DR
Proposed Solution must support all required features to be handled by a SINGLE endpoint agent
Proposed Solution must perform all monitoring and block activities at the endpoint; continuing to perform those actions irrespective of if User is connected to internal / private / VPN network or offline (Only Blocking) and store the logs offline and send to the server once its connected back
All Modules of the Proposed Solution must be centrally configurable from central management dashboards
Proposed solution should be password protected from being uninstalled and should be tamper proof
Proposed Solution should be able to implement temporary policies for uplifting the user privileges for a defined duration
Proposed solution should support Sub-Admin Accounts with different privileges/user groups/views and different User Groups
Proposed Solution should support integrations with Microsoft Active Directory; for scheduled Sync of organization and User information
Proposed Solution should support central key management for with Windows Bitlocker
Proposed Solution should support integrations with Data Classification Tools for controlling and monitoring classified data
Proposed Solution should support data export facility for SIEM Solutions
Proposed Solution should be capable of being deployed in Stealth Mode at the endpoints
Proposed Solution should be capable of providing options for Customised Pop-up Messages for any blocked activity
Proposed Solution should offer a globally adjustable Sync Interval for Policy and Log Synchronization
Proposed Solution should offer User/Device level adjustable Sync Interval for Screenshots and Shadow Logs synchronization to manage locations with lower bandwidth
Proposed Solution should support Agent Installation via Manual or Automated (Silent / Verbose) methods
Proposed Solution should Support AD GPO or other third-party solutions for Remote Agent Push
Proposed Solution Console should in real time indicate Agent Connectivity Status, last connected time and Agent Version
Proposed Solution should support future agent update deployments via the Console
Proposed Solution should also support a CSV based Organization / Group / User Information imports and manual Workgroup User Creation
Proposed solution must support LDAP based authentication mapping for Admins & Sub-Admin accounts
Proposed solution musts have 2FA for Administrator login and password enforcement for admin and subadmin logins and automatic period based pass expiry
Proposed solution must store all information in encrypted form and should implement AES 256 encryption in data storage at endpoints. Solution should enforce TLS 1.2
The solution should allow user to define a single set of policies once and deploy across all products.
The DLP Solution should automatically notify data owners of this policy violation.
The solution should have a comprehensive list of pre-defined policies and templates to identify and classify information pertaining to Banking and Finance vertical and India IT act.
The solution should enforce structured and unstructured fingerprint policies even when disconnected from corporate network. The endpoint would be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact and network components to reduce WAN overheads.
The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information

copied to removable media. It Should support both Native and Portable Encryption and manage the Encryption and DLP policies from the same management Console.
The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident
The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint
The system should display the original file location and policy match details for files found to violate policy
The unavailability of a management component/ server in no way shall impact the functioning of a client.
The OEM should have own technical support center in India.
The solution should support watermarking for all documents with IP Address printed from the end points.
The solution should support enforced encryption on content transfer through CD/DVD and also support CD/DVD writer whitelisting.
The solution should have pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste & File Access. Also, solution should have the capability to define the third-party application. The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files.
The solution should monitor sensitive content accessed by cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud.
Solution should ensure blocking of Windows / Non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information copied to removable media. It should support both Native and Portable Encryption and manage the Encryption and DLP policies from the same management Console.
Monitoring and Reporting
Proposed Solution should be able to Monitor, Shadow Log and generate alerts for sensitive files being uploaded through different applications.
Proposed Solution should have a highly customisable Incident rule creation interface; that allows for each incident to be tagged to avenues of impact (Data Loss Potential, IT Misuse etc), while being able to assign a High / Medium / Low severity for the Incident.
Proposed Solution should have Dashboard Notifications for each Incident or Violation
Proposed Solution should have automatic Email Alerting for each incident real time
Proposed Solution should have the automatic email alerting for Daily Summary of Incidents each day
Proposed Solution should have a Summary Incident Dashboard for easy referral of organisation level User Behaviour Assessment
Proposed Solution Incident Summary Dashboard should detail counts of each violation and also a comparative analysis of previous period performance vis-à-vis present period performance
Proposed Solution should have inbuilt Scoring Matrix and a reporting mechanism that is automated to run analytics based on number of incidents, avenue and severity of Impact
Proposed Solution Should be able to calculate and display Organisation Compliance Score based on Policies set for Data Loss Prevention internally to the platform
Proposed Solution be able to calculate and display Organisation Data Protection Score based on number of Incidents with Data Loss Potential and severity of Impact
Proposed Solution be able to calculate and display Organisation Productivity Score based on number of Incidents with Productivity Loss and severity of Impact
Proposed Solution Should Have an Executive Dashboard that summarises overall organisational health scores and areas of concern
Proposed Solution's Executive Dashboard should provide easy navigation and drill down capabilities to investigate areas of concerns - department, region, zone to user level.
Proposed Solution should isolate and centralise visibility of risky users and malicious activities to Executive Committee
Proposed Solution should be able to generate detailed incident forensics report
Proposed Solution should do activity tracking of Users and Devices across all activity channels
Proposed Solution should log all relevant details where applicable in each channel for forensic investigations and audits; including but not limited to Device ID, User ID, Application, URL, Website Category, Files accessed, Files Transferred, File Names, File Sizes, Printer ID, Network Connectivity Details, Email from / to/ cc/ bcc/ subject/ body/ attachment
Proposed Solution should be capable of Filtering Activity Reports by User / Or by Device

Proposed solution should be capable of Daily/Monthly consolidated view and Analytics of various Productive and Unproductive activities of Single/All Agent/Agent Group Wise as well as Single/All User/ User Group Wise
Proposed solution should be capable of Daily/Monthly Login and Logout Reports, Analytics of Single/All Agent and Agent Group Wise as well as Single/All User Group Wise
Proposed solution should be capable of Daily/Monthly Analytics Reports on the basis of Active, Idle, Productive and Unproductive Screen time spent by All/individual Agent/Agent Group as well as All/Individual User/User Group
Proposed solution should be capable of Daily/Monthly Analytics, Reports on basis of Productive and Unproductive Application Used by All/Individual Agent/Agent Group as well as All/Individual User/User Group
Proposed solution should be capable of Daily/Monthly Analytics, Reports on basis of Productive on and Unproductive Websites accessed by All/Individual Agent/Agent Group as well as All/Individual User/User Group
Proposed solution should be capable of Productive Activities Unproductive Activities Group-wise Reports Daily/Monthly Reports
Proposed solution should be capable of generating Daily Utilization Web Browsing Login Logout, Daily Productivity Summary Reports - Agent Wise as well as User Wise, Daily Application Utilization Reports - Agent wise as well as User Wise, Daily Web Browsing Activity Reports - Agent wise as well as User Wise, Weekly Worktime Profile Reports (Reflector Reports) - User Wise
Proposed solution should be able to take periodic screenshot to monitor detailed employee activity for forensic evidence
Proposed Solution should be able to graphically represent productivity of the users.
Proposed Solution should also log and support audit of all Admin and Sub-Admin Activities
Proposed Solution should support extraction of Raw Data Logs or Filtered Reports via CSV/ PDF formats
Proposed Platform should be capable of generating Alerts on any Policy Changes or Agent Uninstallation / Deletion performed by an Admin or a Sub-Admin
Proposed Solution should support Policy Setting as well as Reporting separately for Devices and Users
Proposed solution should have Account lockout policy in which after certain unsuccessful attempts user will not be able to login the dashboard without Master Admin's intervention
The solution should provide built-in reports and dashboards to analyze user behavior and system health.
The solution should integrate with third-party reporting tools to provide meaningful reports on user activity and deployment.
Water Marking
The system should generate watermark on the files which are printed automatically and can be customised according to admin requirement
Files supported content to be printed should be selectable by the admin eg. PDF, Word, Images etc.
Must provide config option to customise the appearance & placement of the watermark on the printed files.
Data Discovery
Proposed Solution should have the ability to run Data Discovery at endpoints at one time and incremental level
The solution should be able to discover and audit sensitive data at rest in the network or in the end user machines.
The solution should provide a built-in dashboard for reviewing data discovery scanning results for user activity, deployment, data storage trends.
The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes
The solution should provide the ability to run scheduled scans to automatically classify files based on several factors, including the file properties/attributes, content, and/or metadata.
The system should display the original file location and policy match details for files found to violate policy
The system should support incremental scanning during discovery to reduce volumes of data to be scanned.
The solution should be capable to discovers and locate confidential information in network and cloud storage repositories, on file and web servers, databases, and endpoint devices.
The Solution should have advanced policy capability – Ability to learn sensitive information from copies of information that needs to be protected for various data channels (e.g. Endpoint, Network, Cloud, Web & Email)
The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients.
The reports should be exported to at least CSV, PDF, HTML formats.

The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console.
The solution should allow a specific incident manager/team member to manage incidents of specific policy violation, specific user groups etc.
The system should allow automatic movement or relocation of file during discovery and protection.
The system should allow automatic movement or relocation of file, during discovery.
Solution should support for various data masking techniques, such as substitution, shuffling, encryption, and nulling out.
The solution should support scheduled scan to discover data at rest.

16. Detailed specifications of NAC Appliance with AAA

S. No.	Parameter	Specifications/ Values	Complaint Yes/No
1.	Deployment Form Factor	Hardware appliance or VM with centralized and distributed deployment support	
2.	Supported Endpoints	Minimum 5,000 devices (scalable to 50,000+ with clustering)	
3.	AAA Support	Built-in RADIUS and TACACS+ support	
4.	802.1X Authentication	Must support 802.1X (wired/wireless), MAB, web auth	
5.	Directory Integration	Must integrate with LDAP, Active Directory, RADIUS external DBs	
6.	Endpoint Profiling	Automatic device identification using DHCP, SNMP, MAC OUI, HTTP headers	
7.	Guest Access Management	Captive portal, guest self-registration, sponsor approval	
8.	BYOD Support	Onboarding workflows for personal devices, including certificate provisioning	
9.	Policy Engine	Rule-based policy with context-aware access controls	
10.	Posture Assessment	Integration with antivirus/patch posture checks	
11.	Quarantine/Remediation	VLAN switching, dACL, CoA, or redirection for non-compliant devices	
12.	Integration with Security Tools	SIEM, SOAR, firewall, MDM, threat intel (via pxGrid/API)	
13.	Cluster/High Availability	Multi-node deployment with failover	
14.	Management Interface	Web UI + CLI + API (for automation and integration)	
15.	Compliance & Certifications	FIPS 140-2, Common Criteria, ISO 27001, GDPR, PCI DSS	

16.	Virtualization Support	VMware, Hyper-V, KVM, and public cloud (optional)	

17. Detailed specifications of Patch Management server

Patch Management	
Sl. No.	**Minimum Technical Specifications**
1.	Shall be a multi-platform application / system with support for Windows (Desktop, Server) and Linux (Ubuntu, Debian, Centos, Redhat)
2.	Automatically scans the endpoints to find the missing patches
3.	Solution should have functionality to downloads the required patches for deployment
4.	Shall support Customized Deployment Window/ scheduling of patches for the deployment
5.	Shall support to download and keep the patches in client machine before the deployment window, so that deployment window can be used effectively.
6.	Automatically installs the missing patches to endpoints as per the configured task
7.	Shall support Customized Reboot Policy
8.	Shall support to enforce reboot from Central Console after a period of time
9.	Shall support all types of Microsoft updates which includes Feature Pack, Cumulative, Rollup, Preview, Optional, etc,
10.	Shall support Security Updates for different Linux Flavours (Ubuntu, Debian, Centos, Pardus, Redhat and SUSE)
11.	Shall support patch management of major Third-Party application for Windows, MAC and Linux
12.	Shall support various predefined reports with extensive filter options
13.	Shall support scheduling the reports to multiple mail address
14.	Shall support creating custom report with available data
15.	System shall support configuration for calculating the client health based on different parameter like Severity, Patch Approval,
16.	Shall support to automate the patch testing process in your test environment
17.	Shall support to automatically approves the patches based on the patch deployment status in test machines
18.	Shall support creation of machines group for better management
19.	Shall support creation of dynamic group based on different parameters like System Type, Operating System, etc.
20.	Shall support cleanup of the Patch Store regularly for managing the disk space
21.	Shall support Failover server for zero downtime of Server. The server shall be installed in HA mode.

22.	All the hardware, software and licenses required to run the system shall be part of the bid.
23.	Shall support setting up of jump server to create an air-gapped environment for downloading the patched required to be installed in the network
24.	Shall provide API's to export data to different tools as required and also to perform various actions like integration with other systems
25.	Support integration with NAC server to enable automatic patching to make the system compliant before joining the network. For that NAC and Patch Management should be from same OEM
26.	Define Role based User Administration
27.	Supports SAML Authentication
28.	Supports two/multi factor authentication, from same OEM, to make sure the integrity, Tool should be securely accessed, with capability inherently built in the system, so to have secured access as a legacy capability. this should be available from day zero, with tightly couple architecture, such that application works smoothly. external integration should not be done
32	Solution from an OEM that is CMMi LEVEL 3. Certification copy for the same to be submitted along with bid submission
33	The proposed solution must be an industry standard solution from an OEM that is ISO 20000, ISO 27001:2013, ISO 14001:2015, ISO 9001:2015, ISO 15408-1:2005, & ISO 27034-1:2011 to ensure the quality and security. Certification copy for the same to be submitted along with bid.
34	The proposed solution should be secured with single sign-on (SSO) and must have authentication through LDAP. For enhanced security and effectiveness Patch Management, SSO engine & LDAP solution should be from the Same OEM
35	The proposed solution should have deployment reference at least 5 deployments with minimum 5000 end points reference in Indian Govts. Documentary proof must be submitted along with bid.
36	The proposed solution should be 100% Make in India. IP Rights should be available with the vendor and reside in India

18. Detailed specifications for Windows 2022/2025 STD 16 Core

Parameter	Specification
Product Name	Microsoft Windows Server 2022 Standard / Windows Server 2025 Standard
Edition	Standard
License Type	Per Core (16-Core Base License Pack)
Version	Latest release (2022) or upcoming (2025) with downgrade rights (if applicable)
License Validity	Perpetual
License Model	16-core pack; must cover minimum of 16 cores per physical server
CAL Requirement	Requires Client Access Licenses (CALs) separately for users or devices
Deployment Type	Physical or Virtual (up to 2 VMs per license with Hyper-V rights)
Virtualization Rights	2 Operating System Environments (OSEs) or Virtual Machines (VMs)
Hypervisor Support	Includes rights to run Microsoft Hyper-V role

File System Support	ReFS (Resilient File System), NTFS, FAT32
Supported Hardware Architecture	x64-based hardware (minimum 1.4 GHz, 64-bit processor with compatible chipsets)
Minimum Hardware Requirements	1.4 GHz 64-bit processor, 512 MB RAM (2 GB for Server with Desktop Experience), 32 GB storage
Max Hardware Support (Standard)	Up to 24 TB RAM and 64 sockets (actual depends on OEM hardware)
Core Features	Active Directory, DNS, DHCP, Group Policy, Failover Clustering, Hyper-V, Windows Admin Center
Security Features	TPM 2.0 support, Windows Defender ATP, Credential Guard, Secure Boot, BitLocker
Networking Features	SDN, Network Controller, DNS Policies, TCP Fast Open, SMB over QUIC (2022), Secure DNS (2025)
Management Tools	Windows Admin Center, PowerShell 5.1/7.x, Group Policy Management, Server Manager
Storage Features	Storage Spaces Direct, Deduplication, Tiering, Storage Replica (limited in Standard)
Cloud Integration	Azure Arc Ready, Azure Hybrid Benefit, Azure Stack HCI compatible
Language Support	Multilingual; includes English and other Indian/UN official languages via MUI
Media Delivery	Digital License Key (e-License) or Physical Media (DVD/USB optional)
Compliance & Certification	BIS, ISO 27001, Common Criteria EAL4+, FIPS 140-2 validated modules
OEM Eligibility	Must be licensable via OEM, Volume License (Open Value), or Cloud Solution Provider (CSP) model
Support Lifecycle	5 years mainstream + 5 years extended support (from release date). Minimum support should be as per as per Hardware WARRANTY AND Software Support clause defined in point M of this document
OEM Brands Supported	Dell, HPE, Lenovo, Cisco UCS, Supermicro, Acer, Fujitsu, etc.

19. Detailed specifications for RHEL 9.5 1-2 Socket Lic Virtual

Parameter	Specification
Product Name	Red Hat Enterprise Linux (RHEL) 9.5
Edition / SKU	RHEL Virtual Datacenter / Virtualization Subscription
License Type	Subscription-based (Annual or 3-year preferred)
Socket Licensing	Supports 1–2 physical sockets in the virtualization host (hypervisor)
Deployment Type	Virtual Machines only (Hypervisor required: KVM, VMware, Hyper-V, etc.)
Virtual Guests Supported	Unlimited virtual machines on the licensed host
Architecture Supported	64-bit x86_64, ARM (where applicable)
Kernel Version	Kernel 5.14+ (for RHEL 9.5)
System Requirements	- CPU: x86_64 (1.1 GHz or higher) - RAM: ≥1 GB (minimum), ≥2 GB recommended
Key Features	SELinux, SystemD, Cockpit GUI, firewalld, containers (Podman), tuned profiles, Image Builder

Security Features	- FIPS 140-3 validated modules - SELinux (enforcing) - Secure Boot, Role-Based Access
Virtualization Optimization	Enhanced KVM support, performance-tuned kernel, para-virtualized drivers
Management Tools	RHEL Web Console (Cockpit), Red Hat Insights, Satellite integration (optional)
Container Tools	Podman, Buildah, Skopeo (no Docker required), compliant with OCI standards
Software Lifecycle Support	10 years (5 years full + 5 years extended lifecycle). Minimum support should be as per as per Hardware WARRANTY AND Software Support clause defined in point M of this document
Update Mechanism	yum/dnf based package management with access to Red Hat repositories
Subscription Includes	- Access to official RHEL 9 repositories - Unlimited updates & patches - Security errata
Support Model	9x5 Standard or 24x7 Premium support (based on selected tier)
Cloud Readiness	Azure, AWS, Google Cloud certified images available (if hybrid/cloud infrastructure needed)
Certification & Compliance	Common Criteria EAL4+, FIPS 140-3, ISO 27001-ready, STIG-aligned baselines available
OEM Compatibility	Compatible with HPE, Dell, Lenovo, Cisco UCS, Supermicro, VMware, Oracle VM, KVM
License Delivery	Digital entitlement via Red Hat Customer Portal

20. Detailed specifications of AIO

Sl. No.	Parameter	Specifications/ Values	Remarks
1.	Processor	Intel Core i7 (13th Gen or higher), ≥4 cores, ≥8 threads	
2.	Base Clock Speed	≥3.5 and ≤ 4.9 GHz with Turbo Boost	
3.	RAM	Minimum 16 GB DDR4/DDR5, upgradeable to 64 GB	
4.	Storage	512 GB SSD (NVMe M.2) with additional SATA slot (optional)	
5.	Display	23.8" FHD IPS (1920×1080) anti-glare, ≥250 nits	
6.	Webcam	5MP or higher with privacy shutter, IR support preferred	
7.	Graphics	Integrated Intel UHD or Iris Xe Graphics	
8.	Ports	Minimum 6 USB ports (at least 2 USB 3.2 Gen 2), HDMI, LAN, Audio Combo	
9.	Ethernet	10/100/1000 Mbps RJ45 LAN	
10.	Wireless	Wi-Fi 6 or 6E + Bluetooth 5.2 or higher	
11.	Security	TPM 2.0, Secure Boot, BIOS-level password protection, DriveLock	
12.	OS Preload	Windows 11 Pro 64-bit Licensed	

Sl. No.	Parameter	Specifications/ Values	Remarks
13.	Stand Adjustability	Tilt + Height adjustable stand	
14.	Keyboard/Mouse	USB or wireless combo included	
15.	Power Supply	External/Integrated 90W or higher	
16.	Form Factor	Compact AIO (≤60 mm depth)	
17.	Certifications	ENERGY STAR, EPEAT Gold, RoHS, TCO Certified	

21. High End PC SPECIFICATIONS

Description of Parameters	Minimum Acceptable range or Parameters
Processor Make	Intel /AMD
Processor Description	Intel Core i7 13,700 with minimum 5.20 GHz Max/ AMD Ryzen 9 7900
Processor Generation	13th generation or higher or equivalent AMD 9 generation
Chipset	Q670 or equivalent AMD
Graphics type	Integrated
Monitor size	23.0" or more
Monitor type	IPS panel with full HD resolution (1920 x 1080) or better
Operating system	Windows 11 professional Licensed
Memory	32 GB upgradeable to 64GB with 2 DIMM slots
Hard disk capacity	1 TB PCIe NVMe SSD and it should be upgradable up to 2 TB SSD
Ports	Headphones and microphone ports or headphone/ microphone combo jack (universal audio jack)
	1x Ethernet (RJ-45) minimum
	1x HDMI
	1x Wi-Fi enabled minimum
	1x Type C port minimum
	Min 3 USB ports of 10 GBPS with 1 HDMI output
Built in webcam	FHD webcam min 5 MP or higher
Internal speaker	2X 2W
Keyboard	Wired from the same OEM as the main unit
Mouse	Wired from the same OEM as the main unit
On site OEM warranty	As per Hardware WARRANTY AND Software Support clause defined in point M of this document
Additional requirement	Pre-loaded windows 11 professional Licensed
	Latest version of Ms. Office perpetual Licensed

22. Cyber Threat Intelligence (CTI)

- The solution shall be provided as a platform-based service enabling acquisition, monitoring, analysis, and dissemination of cyber threat intelligence.
- The platform shall support integration with existing SOC/SIEM/SOAR/EDR/TIP solutions using standard protocols such as STIX/TAXII, API, JSON, XML, CSV.
- **The solution shall have access to a wide range of intelligence sources (surface web, deep web, dark web, encrypted channels, social media platforms, etc.) with a repository of at least:**
  - 5 billion or more threat artifacts (IOCs, IOAs, TTPs).
  - 9 billion or more compromised credentials.
  - 9 million or more threat actor profiles.
  - 300 million or more indexed records from dark web sources.
- **The platform shall provide real-time and near real-time monitoring with configurable filters for improved accuracy and targeting.**
- **The solution shall provide repositories for:**
  - Data breaches and compromised credentials.
  - Compromised payment and identity data.
  - DNS records, IP reputation, and malicious network activity.
  - Threat actor profiles and associated campaigns.
- The platform shall support multi-language translation (minimum 40 languages) in offline mode to ensure confidentiality.
- The solution shall include case management functionality to allow secure collaboration and tracking of threat investigations.
- The system shall generate executive-level reports and provide automated alerts via email and SMS.
- The platform shall include AI-driven risk and attack surface monitoring capabilities to identify and score risks across external, internal, and cloud environments.
- The solution shall cover the following threats and risks:
  - Account Takeover (ATO), Business Email Compromise (BEC), botnet infections.
  - Brand abuse, cybersquatting, and fraudulent domains.
  - Data breaches, credential leaks, and dark web activity.
  - Exposed or misconfigured cloud/network services.
  - Vulnerable or unpatched applications and infrastructure.
- **The platform shall provide threat risk scoring with actionable remediation intelligence.**
- **The system shall offer detailed reporting and contextual awareness to prioritize high, medium, and low-risk threats.**
- **The solution shall support cloud workload monitoring (minimum AWS and Azure) for continuous security posture evaluation.**
- **The bidder shall provide professional services including:**
    - Threat intelligence collection, analysis, and dissemination.
    - Training and awareness sessions (online/onsite) for stakeholders.
    - Proactive threat hunting operations.
    - Red teaming, vulnerability assessment, and penetration testing.
    - Digital footprint monitoring of brand, domains, DNS, and user assets.
    - Remediation and takedown support for malicious/fraudulent content.
- **The solution shall support deployment flexibility – on-premises or in-country cloud (SaaS) as per customer requirements.**
- The bidder shall provide 24x7x365 technical support through secure communication channels (phone, email, ticketing).
- The solution shall comply with relevant national regulations and international cybersecurity standards

ANNEXURE 'B'

Minimum Baseline Device Hardening Measures

(i) Firewall Hardening Measures

a) Periodic OS/Firmware updates, patch update and management to be ensured.
b) Strict whitelisting-based rules for VLAN-to-VLAN communication.
c) Filter rules restricting destination addresses, ports, services, and protocols.
d) Block clear-text protocol services.
e) Logging of all deny statements in ACL.
f) Configure IPSec VPN with tunnel mode.
g) Secure management connections (FIPS 140-2 standards), timeout, and logging.
h) SNMP access control, disable insecure SNMP versions and default communities.
i) Disable unnecessary services and default accounts.
j) Implement strong password policies.
k) SSH session timeout set to 60 seconds, attempts limited to 3.
l) Prevent half-open connections, disable auxiliary ports.
m) Block loopback addresses, Teredo tunnelling, and restrict IPSec traffic.
n) Emergency admin accounts with privilege controls.
o) Block outbound management traffic, enable NTP authentication.
p) Use strong encryption (TLS, 128-bit ciphers).
q) Log all network filter rules and enable additional logging fields (domain/url, utm-action, statistical logs).
r) Block teardrop, SYN flood, and enforce session timeouts.
s) Disable HTTP services if not required; prefer HTTPS.
t) Avoid PAT where possible.
u) Synchronize logs with NTP.
v) Enable IDS/FW alarms for admin notifications.
w) Block loopback traffic and implement ACL restrictions on server VLANs.

(ii) Layer-3 Network Device Hardening Measures

a) Periodic OS/Firmware updates, patch updates.
b) Inbound/outbound ACLs for valid source/destination addresses.
c) VRF bound to appropriate interfaces.
d) Default-deny policy with allow by exception.
e) Drop IPv6 packets with invalid headers or options.
f) Key duration for routing protocols not to exceed 180 days.
g) Block IP options, enforce TTL propagation.
h) Block outbound management traffic, allow only authorized communications.
i) Implement control-plane protection and disable zero-touch deployment.
j) Management via IPSec tunnels and OOBM interface only.
k) Maintain audit logs identifying event sources.
l) Disable auxiliary ports, LLDP, inactive interfaces.
m) Log dropped packets and stop forwarding on critical failures.
n) Disable vendor call-home features.
o) Enforce OSPF strong authentication and priorities.
p) Disable SNMPv1/2 or configure SNMPv3 with secure settings.
q) Disable DTP, CDP, ICMP redirects, ARP proxying, classless routing, IP unreachable, protocol forwarding.
r) Secure session timeouts and disable Telnet.

s) Configure central SIEM logging.
t) Enforce minimum password complexity and length.
u) Restrict NTP access, secure SNMP access.
v) Implement port security, VTP in transparent mode.
w) ACLs to restrict administrative service access.
x) Disable MOP protocol.
y) Enforce compliance with NTRO IS policy for user credentials.

ANNEXURE 'C'

(Minimum Baseline Capabilities of NOC/SOC setup)

1. SOC should be configured to have following capabilities;

(a) Device Agnostic i.e capable of ingesting logs of devices with different make, model, log format and functionality across the ICT infrastructure with built-in parsers.

(b) Customized dashboard features facilitating reporting mechanism as per operational requirements.

(c) Central Cyber Threat Intelligence (CTI) platform as an input to SOC and Central Data Lake for AI/ML & correlation. Mentioned CTI should be compatible for receiving inputs (in terms of IoCs, TTPs etc.) from commercial, open or any other closed group sources in vide range of formats like json, csv, txt, STIX etc.

(d) Entire SIEM / SOC should have redundancy control and fail-safe mechanism in place.

(e) Enrichment capabilities like geo-ip, threat attributes, asset tagging, whitelisting etc.

(f) **Annexure- 'D'** may kindly be referred for advance level use cases incorporating AI/ML Algorithms for generation of unknown threat actors. As an indicative input Firewall/UTN, DNS and WAF are considered at the moment. Similar threat models need to be articulated by bidder/contractor for other ICT infrastructure along with MITRE ATT&CK mapping.

2. The following functionalities should be configured on the SOC dashboard for enhancing the efficiency of SOC:

(a) Risk manager component to be added/activated in SIEM for generating alert for vulnerabilities in Software/Applications/Firmware used in the entire IT stack through updated SBOMs (Software Bill of Materials).

(b) Monitoring of privileged user/ administrator and important user accounts with regards to successful, failed logins and off-time logins. Generate alerts for anomalies.

(c) Monitoring of successful logins to user accounts beyond office working hours and generate alerts for accounts from which this activity is observed beyond a pre-defined threshold (recommended value 10).

(d) Monitoring and alert for repeated lockouts and authentication failure attempts.

(e) Monitoring of external connections to sites/ destinations that are denied as per the security policy of Network.

(f) Suitable alerts should be configured for timely detection of successful/ failed logins for one user accounts from two different locations/ hostnames within pre-defined time interval.

(g) Alert for any access attempts, successful login and failure to any Networking devices and their configuration changes from non-whitelisted machines.

(h) Monitoring of windows event logs of all the client machines for setting up alerts in respect of violations to the Bonafede usage i.e Acceptable Use Policy (AUP) like what the users can or cannot do on their IT assets while configuring and managing devices and networks.

(i) Set up alert for any traffic originating from unallocated IP in the allocated IP range to any host machine/ network device. Any traffic from non-whitelisted IPs in Network may trigger an alert in SIEM/SOC.

(j) Monitor for assets not being connected to the network for prolonged duration and suddenly trying to communicate with the central site. Generate alerts for such activity.

(k) Ensure that the practice of incident ticket management is implemented and strictly adhered to by all SOC team members. All tickets for incidents should only be closed after the facts have been verified.

(l) Ensure that proper time bound investigation of every alert is undertaken.

(m) For every alert generated by the SOC, ensure that the corresponding raw event log and packet capture logs that triggered the alert, is also available for investigation.

(n) Suitable alerts should be configured for timely detection of network/service enumeration attempts.

(o) Usage of AI/ML components for triggering alerts in respect to beaconing/robotic and rarity-based anomalies in the network should also be configured.

(p) Inbuilt Asset management and Monitoring Tool to pin-point the shadow or rogue devices (if any) in addition to uniformity in the cyber security configurations and compliance from central location.

(q) SOC should also be able to identify the continuity in log sources and should be able to pin-point and raise alert in case of discontinuation or disruption in log feeding sources like sensors, N/W devices, UTM/FW etc.

(r) All the remote connections to be captured along with executed commands by the OEM/SI. Inbuilt threat models to raise alert, if there is any deviation in the whitelisted commands.

(s) Capability for Cyber Kill Chain mapping with respect to network systems.

(t) MITRE ATT&CK or D3FEND mapping in SOC platform with respect to triggered alerts.

(u) Protocol based threat alert analytics and alert generation capability for abnormal, rare or vulnerable version of protocol usage with support of AI/ML/DL algorithm for baselining on large and historical data sets.

(v) Some baseline event-Ids (for windows) to be monitored in the SOC in respect to all the systems/servers for ruling out any intrusion/abnormality is enclosed at **Annexure – 'E'.** The list is indicative only and not exhaustive. Similarly, approach should be followed by bidder/contractor for Linux, Mac based or any other customized/proprietary OS also.

3. Following data from endpoints is required to be fed & analyzed in SIEM / SOC data lake.

- List of Running services
- Parent-Child Process Trees
- Integrity hash of background executables
- Installed applications
- Local and domain users
- Unusual authentications
- Nonstandard formatted usernames
- Listening ports and associated services
- Domain Name System (DNS) resolutions
- Settings and static routes
- Established and recent network connections

- Run key and other autorun persistence
- Scheduled tasks
- Artifacts of execution
- Event logs
- Antivirus detections
- Operating system logs-Sysmon, WEF, Syslog, SNMP, WMI, Powershell
- Firewall, UTM, WAF and DNS Debug Logs
- Volatile Artifacts- Temporary artifact collected from endpoint data sources for the purpose of hunting that might not touch the disk on the host Data Collection: Memory, Network Conn, Process Conn
- Non-Volatile Artifacts: Artifacts that reside on endpoint / hot disk
- Data Collection: Prefetch, Amcache, Shimcache, MFT, Registry, bash_history, Task Scheduler

4. (a) Log Sources at each vertical: SOC shall be capable to collect logs from all systems, devices, applications, services etc. deployed in the verticals. For example: Switch/Router/IDS/IPS/Firewall, WAF, DNS, Windows, Linux, AD Access logs, AAA, proprietary software/applications etc.

(b) The required data which is required to be ingested, processed and converted in meaningful intelligence should be clearly mapped to HW and SW requirements.

(c) Secure architecture deployment for SOC with complete security controls in place as per the benchmarks like CIS.

(d) Proper encryption mechanism may be provided in respect of log data being collected from various sites.

(e) Tentative Timeline to resolve critical application issues may be specified by bidder/contractor.

(f) Time synchronization of the entire logs pushed in SOC should be in place for coherent analysis. Dedicated NTP server with backup should be in place so that time of ingestion and time of event should be uniform across all devices for effective analytics and cyber kill chain mapping (if any).

Annexure-'D'

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
DNS	I. Excessive number of DNS NXDOMAIN responses on internal sub-domains II. Excessive number of DNS SERVFAIL responses on Internal sub-domains III. Excessive number of failed DNS zone-transfers. IV. Possible fast flux domain detected. V. Persistent traffic to rare non-resolvable domain dns responses. VI. Rare dns host resolved. VII. Rare dns server used. VIII. Randomly generated domain detected on dns response. IX. Beaconing traffic to rare domains over dns The following additional use can be achieved provided the event logs for these activities are being received. X. DNS response conflicts/cache alteration XI. DNS failed access attempts / brute force XII. Root/admin command execution XIII. Privilege escalation XIV. Access trends deviation XV. Open resolver check	✓ Severity ✓ Class-Name ✓ Outcome ✓ Category ✓ HostAddress ✓ Category ✓ SourceIP ✓ SourcePort ✓ Service ✓ Datetime ✓ DestinationHost ✓ Transaction ✓ Action ✓ IPAddress ✓ Type_Name ✓ DeviceAddress ✓ Protocol ✓ Query /Rsponse (Q/R) ✓ Domain Requested ✓ Flags (hex Value)	Requisite attributes are available with DNS Debug logs

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	XVI. TPI linkages for IOCs/phish etc.		
Firewall	I. Abnormal amount of data aggregated from FTP ports – Firewall II. Abnormal amount of data aggregated from SMB ports – Firewall III. Abnormal amount of data transmitted from DNS ports – Firewall IV. Abnormal amount of data transmitted from known file transfer ports – Firewall V. Abnormal amount of data transmitted over covert channels – Firewall VI. Abnormal number of connections on LDAP ports – Firewall VII. Abnormal number of connections on SMB or NETBIOS ports – Firewall VIII. Abnormal number of connections on Telnet ports – Firewall IX. Abnormal number of DNS zone transfers – Firewall X. DNS amplification by frequency of packets – Firewall XI. Firewall traffic to randomly generated domains – Firewall	✓ Applicationprotocol ✓ baseeventid ✓ bytesin ✓ session status ✓ destinationaddress ✓ destinationport ✓ ipaddress ✓ accountname ✓ transportprotocol ✓ message/signature ✓ destinationhostname ✓ categoryoutcome ✓ eventtime ✓ date/time ✓ action take by firewall ✓ bytes sent ✓ bytes received ✓ URL accessed ✓ Transport-protocol ✓ Statistical log attributes viz sent-delta & receive-delta ✓ Source interface ✓ Destination interface ✓ UTM action ✓ Log type ✓ Log Subtype ✓ Session ID ✓ Source NAT IP ✓ Destination NAT IP	Complete verbosity of the logs required for subject use case development Following types of logs are required: (a) Traffic (b) Threat (c) Web-Filtering (d) Antivirus (e) IPS / IDS (f) VPN

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	XII. Possible external host enumeration over system ports – Firewall XIII. Possible external port scan over system ports – Firewall XIV. Possible host enumeration over system ports – Firewall XV. Possible lateral movement over network traffic – Firewall XVI. Possible port scan over system ports – Firewall XVII. Rare application for known protocols on network traffic – Firewall XVIII. Rare port used by applications on network traffic – Firewall XIX. Traffic to rare domain on DNS ports – Firewall XX. Traffic to rare server on DHCP ports – Firewall XXI. Beaconing traffic to malicious IPs/Domains/CnCs over firewall XXII. Rare port used by applications on network traffic XXIII. Rare application for known protocols on network traffic The following additional use cases can be achieved provided the event logs for these activities are being received. XXIV. HTTPS traffic over non-https port		

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	XXV. Firewall access logs anomalies XXVI. Dictionary attack/Brute force attempts XXVII. Multiple sources making session request for an account – In a given timeframe from sources like windows, unix and from different countries /geographic locations/IPs (Land-speed Detection) XXVIII. One IP and respective session associated with more than one user ids XXIX. Destination Sweeper in mean time – Threshold of IPs to be set. XXX. Fire-walking or Host sweeper XXXI. Excessive inbound/outbound connections from same source. XXXII. DOS/DDOS – If particular number of packets blocked by Firewall/UTM. XXXIII. VPN two or more country login within say 1 hr by same user. XXXIV. Privilege escalation observed from the same IP (i.e elevation to root or admin)		

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	XXXV. Account logins at unusual hours		
WAF	I. Abnormal number of high severity alerts II. Malicious URLs or OWASP based web application attacks. III. Application based CVE vulnerability exploits with continuous signature update mechanism IV. Rare ports used by a process for high severity endpoint alerts Vulnerable Endpoint monitoring V. Infected Endpoint monitoring Virus and Malicious Code Outbreak VI. Detection of a Virus or Malware The following additional use cases can be achieved provided if relevant signatures are logged and forwarded to. VII. Dictionary attack/Brute force attempts VIII. Multiple sources making session request for an account – In a given timeframe from sources like	✓ Category severity - Severity of alert identified ✓ Category behavior - Type of alert identified - DoS/ SQLietc ✓ Device action - Action taken by the device eg: Allowed / Blocked ✓ Destination-process-name - If applicable ,associated processes with the network connection ✓ Destinationport ✓ Signature Description of signature	

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	windows, unix and from different countries / geographic locations/IPs (Land-speed detection). IX. One IP and respective session associated with more than one user ids. X. Destination Sweeper in mean time – Threshold of IPs to be set. XI. Fire-walking or Host sweeper XII. Privilege escalation observed from the same IP (i.e elevation to root or admin) XIII. Account logins at unusual hours		

Annexure-'E'

Windows Event ID(s)

S. No.	Event ID	Description	Remarks
Category: Scheduled tasks			
1)	4697	This event generates when new service was installed in the system.	
2)	106	This event is logged when the user registered the Task Scheduler task.	
3)	4702	This event generates when scheduled task was updated.	
4)	140	This event is logged when the time service has stopped advertising as a time source because the local machine is not an Active Directory Domain Controller.	
5)	4699	A scheduled task was deleted.	
6)	141	The time service has stopped advertising as a time source because there are no providers running.	
7)	201	This event is logged when the task scheduler successfully completed the task.	
8)	4698	A scheduled task was created. The event description contains the user account that created the task in the Subject section. XML details of the scheduled task are also recorded in the event description under the Task Description section and includes the Task Name.	
9)	4699	A scheduled task was deleted. The Subject section of the event description contains the Account Name that deleted the task as well as the Task Name.	
10)	4700	A scheduled task was enabled. See Event ID 4698 for additional details.	
11)	4701	A scheduled task was disabled. See Event ID 4698 for additional details.	
12)	4702	A scheduled task was updated. The user who initiated the update appears in the Subject section of the event description. The details of the task after its modification are listed in the XML in the event description. Compare with previous Event ID 4702 or 4698 entries for this task to determine what changes were made.	
Category: Services			
13)	4688	It documents each program that is executed, who the program ran as and the process that started this process. It is analysed to rule out process injection.	
14)	4697	A service was installed in the system.	

15)	7045	Created when new services are created on the local Windows machine.	
16)	7034	The service terminated unexpectedly.	
17)	7036	The Windows Firewall/Internet Connection Sharing (ICS) service entered the stopped state or, The Print Spooler service entered the running state.	
18)	7040	The start type of the IPSEC services was changed from disabled to auto start.	
Category: Event Log Manipulation			
19)	1102	Whenever Windows Security audit log is cleared, event ID 1102 is logged.	
20)	104	This event is logged when the log file was cleared.	
Category: Authentication			
21)	4776	The domain controller attempted to validate the credentials for an account.	
22)	4771	This event is logged on domain controllers only and only failure instances of this event are logged (Kerberos pre-authentication failed).	
23)	4768	This event is logged on domain controllers only and both success and failure instances of this event are logged (A Kerberos authentication ticket TGT) was requested.	
24)	4769	Windows uses this event ID for both successful and failed service ticket requests (A Kerberos service ticket was requested).	
25)	*4770*	A service ticket was renewed. The account name, service name, client IP address, and encryption type are recorded.	
26)	4771	Depending on the reason for a failed Kerberos logon, either Event ID 4768 or Event ID 4771 is created. In either case, the result code in the event description provides additional information about the reason for the failure.	
27)	4776	This event ID is recorded for NTLM authentication attempts. The Network Information section of the event description contains additional information about the remote host in the event of a remote logon attempt. The Keywords field indicates whether the authentication attempt succeeded or failed.	
Category: Sessions			
28)	4624	An account was successfully logged on.	
29)	4625	An account failed to log on.	
30)	4634 & 4647	User initiated logoff/An account was logged off.	
31)	4648	A logon was attempted using explicit credentials.	
32)	4672	Special privileges assigned to new logon.	

33)	4648	A logon was attempted using explicit credentials. When a user attempts to use credentials other than the ones used for the current logon session (including bypassing User Account Control [UAC] to open a process with administrator permissions), this event is logged.	
34)	4672	This event ID is recorded when certain privileges associated with elevated or administrator access are granted to a logon. As with all logon events, the event log will be generated by the system being accessed.	
35)	4778	This event is logged when a session is reconnected to a Windows station. This can occur locally when the user context is switched via fast user switching.	
36)	4779	This event is logged when a session is disconnected. This can occur locally when the user context is switched via fast user switching. It can also occur when a session is reconnected over RDP. A full logoff from an RDP session is logged with Event ID 4637 or 4647 as mentioned earlier.	
Category: Account Management			
37)	4720	A user account was created	
38)	4722	A user account was enabled	
39)	4723	A user attempted to change an account's password.	
40)	4724	An attempt was made to reset an accounts password	
41)	4725	A user account was disabled.	
42)	4726	A user account was deleted.	
43)	4727	A security-enabled global group was created.	
44)	4729	A member was removed from a security-enabled global group.	
45)	4730	A security-enabled global group was deleted.	
46)	4731	A security-enabled local group was created.	
47)	4733	A member was removed from a security-enabled local group.	
48)	4734	A security-enabled local group was deleted.	
49)	4735	A security-enabled local group was changed.	
50)	4737	A security-enabled global group was changed.	
51)	4738	A user account was changed.	
52)	4741	A computer account was created.	
53)	4742	A computer account was changed.	
54)	4743	A computer account was deleted.	
55)	4754	A security-enabled universal group was created.	
56)	4755	A security-enabled universal group was changed	
57)	4728 / 4732 / 4756	group membership changes.	

58)	4757	A member was removed from a security-enabled universal group.	
59)	4758	A security-enabled universal group was deleted.	
60)	4798	A user's local group membership was enumerated. Large numbers of these events may be indicative of adversary account enumeration.	
61)	4799	A security-enabled local group membership was enumerated. Large numbers of these events may be indicative of adversary group enumeration.	
Category: Network Shares			
62)	5140	A network share object was accessed.	
63)	5142	A network share object was added.	
64)	5143	A network share object was modified.	
65)	5144	A network share object was deleted.	
66)	5145	Network share object was checked to see whether client can be granted desired access.	
Category: Registry Key Values related			
67)	4656	A handle to an object was requested. When a process attempts to gain a handle to an audited object, this event is created. The details of the object to which the handle was requested and the handle ID assigned to the handle are listed in the Object section of the event description.	
68)	4657	A registry value was modified. The user account and process responsible for opening the handle are listed in the event description.	
69)	4658	The handle to an object was closed. The user account and process responsible for opening the handle are listed in the event description. To determine the object itself, refer to the preceding Event ID 4656 with the same Handle ID.	
70)	4660	An object was deleted. The user account and process responsible for opening the handle are listed in the event description. To determine the object itself, refer to the preceding Event ID 4656 with the same Handle ID.	
71)	4663	An attempt was made to access an object. This event is logged when a process attempts to interact with an object, rather than just obtain a handle to the object. This can be used to help determine what types of actions may have been taken on an object (for example, read only or modify data). See Event ID 4656 for additional details.	

Considering the technical complexity and criticality of the project, the evaluation of the bids will be based on **Quality-cum-Cost Based Selection ("QCBS") method as per GFR rules.**

(a) Technical bids will be evaluated for various parameters as specified hereinafter and the technical score secured by bidders in technical evaluation will be considered for further evaluation of bids. Only those responsive proposals that have achieved at least **minimum specified qualifying technical score (50%)** in quality of technical proposal will be considered further for the next stage. Each criterion mentioned under QCBS shall be marked as per the documentary evidence provided by the bidder.

S.No.	Criteria Category	Evaluation Criterion	Max Marks	Supporting Documents Required
A	**Bidder's profile**		**35**	
A1	Average Annual Turnover Average annual turnover over the last three financial years(FY 2022-2023, FY 2023-2024, FY 2024-2025)	(a) More than 200 Crores (10 marks) (b) More than 150 Crores but Less than/Equal to 200 Crores (8 marks) (c) More than 125 Crores but Less than/Equal to 150 Crores (6 marks) (d) Less than/Equal to 125 Crores (4 marks)	10	Certificate from the Statutory Auditor/Company Secretary on turnover details from the over the last three (3) financial years.
A2	<u>Manpower</u> Full time employees on payroll of bidder working in the business unit providing "IT/ITeS" services as on bid submission date	(a) More than 100 (10 marks) (b) More than 50 but Less than/Equal to 100 (8 marks) (c) More than 25 but Less than/Equal to 50 (6 marks)	10	Certificate from the Head of HR Department or equivalent on bidding entity's letter head countersigned by authorized signatory.

		(d) Less than /Equal to 25 (4 marks)		
A3	**Certifications**	ISO 9001 (2 Marks) ISO 27001 (2 Marks) ISO 14001(2 Marks) ISO 20000 (2 Marks) ISO 45001 (2 Marks) CMMi Level 3 or higher (5 Marks)	15	Valid Certificates
B	**Project Experience**		**25**	
B1	The Bidder should have completed projects in IT/ITeS including manpower with minimum value of INR 30 CR and above during last three (3) years as on bid submission date.	(a) More than/Equal to 10 projects (25 marks) (b) Between 6-9 projects (15 marks) (c) Between 3-5 projects (10 marks) (d) Less than 3 projects (5 marks)	25	Work Order + Certificates of Completion (Certified by the Statutory Auditor/Company Secretary).
C	**Technical Presentation**		**40**	
C1	Presentation for understanding of Current requirement as per scope of work, proposed service approach, methodology, work plan for performing the assignment etc.	Technical presentation should cover: • Details of proposed deployment plan, manpower retention strategies and handling of staff resignation including provision	40	Bidder should have to submit detailed Approach and Methodology with Bid document.

		of a backup pool. • Detailed approach & methodology for providing technical support to the project, capacity building for resources and Escalation Matrix. • Proper readable Document submission as well as proper indexing		

(b) After opening and scoring the Financial proposals of responsive technically qualified bidders, a final combined score is arrived at by giving predefined relative weightages for the score of quality of the technical proposal and the score of financial proposal. The scores of the Technical and Financial Bids will be assigned weights as under: **Technical Score: 70%; Financial Score: 30%.** The proposal with the highest weighted combined score (quality and cost) shall be selected.

(c) NCRB reserves the right to modify / amend the evaluation process at any time during the Bid process, without assigning any reason. Any time during the process of evaluation, NCRB may seek specific clarifications from any or all the Bidders. NCRB's decision in this regard shall be final & binding.

बिड संख्या/Bid Number: GEM/2026/B/7361141

दिनांक /Dated: 24-04-2026

बिड दस्तावेज़ / Bid Document

बिड विवरण/Bid Details	
बिड बंद होने की तारीख/समय /Bid End Date/Time	15-05-2026 11:00:00
बिड खुलने की तारीख/समय /Bid Opening Date/Time	15-05-2026 11:30:00
बिड पेशकश वैधता (बंद होने की तारीख से)/Bid Offer Validity (From End Date)	90 (Days)
मंत्रालय/राज्य का नाम/Ministry/State Name	Ministry Of Home Affairs
विभाग का नाम/Department Name	Department Of States
संगठन का नाम/Organisation Name	National Crime Records Bureau (ncrb)
कार्यालय का नाम/Office Name	Ncrb, Nh-8, Mahipalpur
वस्तु श्रेणी /Item Category	Hiring of Agency for IT Projects- Milestone basis
अनुबंध अवधि /Contract Period	6 Year(s)
बिडर का न्यूनतम औसत वार्षिक टर्नओवर (3 वर्षों का) /Minimum Average Annual Turnover of the bidder (For 3 Years)	2500 Lakh (s)
उन्हीं/समान सेवा के लिए अपेक्षित विगत अनुभव के वर्ष/Years of Past Experience Required for same/similar service	3 Year (s)
इसी तरह की सेवाओं का पिछला आवश्यक अनुभव है/Past Experience of Similar Services required	Yes
वर्षों के अनुभव एवं टर्नओवर से एमएसई को छूट प्राप्त है / MSE Relaxation for Years Of Experience and Turnover	Yes | Complete
स्टार्टअप के लिए अनुभव के वर्षों और टर्नओवर से छूट प्रदान की गई है / Startup Relaxation for Years Of Experience and Turnover	Yes | Complete
भागीदारी केवल गवर्नमेंट विक्रेता तक सीमित / Participation restricted to Government seller	Yes (This bid is reserved for participation only by Government sellers and hence Government sellers will be exempted from payment of Transaction charges)
विक्रेता से मांगे गए दस्तावेज़/Document required from seller	Experience Criteria,Bidder Turnover,Certificate (Requested in ATC) *In case any bidder is seeking exemption from Experience / Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer

बिड विवरण/Bid Details	
क्या आप निविदाकारों द्वारा अपलोड किए गए दस्तावेज़ों को निविदा में भाग लेने वाले सभी निविदाकारों को दिखाना चाहते हैं? संदर्भ मेनू है/Do you want to show documents uploaded by bidders to all bidders participated in bid?	Yes (Documents submitted as part of a clarification or representation during the tender/bid process will also be displayed to other participated bidders after log in)
बिड लगाने की समय सीमा स्वतः नहीं बढ़ाने के लिए आवश्यक बिड की संख्या। / Minimum number of bids required to disable automatic bid extension	3
दिनों की संख्या, जिनके लिए बिड लगाने की समय-सीमा बढ़ाई जाएगी। / Number of days for which Bid would be auto-extended	7
ऑटो एक्सटेंशन अधिकतम कितनी बार किया जाना है। / Number of Auto Extension count	2
बिड से रिवर्स नीलामी सक्रिय किया/Bid to RA enabled	No
बिड का प्रकार/Type of Bid	Two Packet Bid
तकनीकी मूल्यांकन के दौरान तकनीकी स्पष्टीकरण हेतु अनुमत समय /Time allowed for Technical Clarifications during technical evaluation	2 Days
अनुमानित बिड मूल्य / Estimated Bid Value	500000000
मूल्यांकन पद्धति/Evaluation Method	Total value wise evaluation
मूल्य दर्शाने वाला वित्तीय दस्तावेज ब्रेकअप आवश्यक है / Financial Document Indicating Price Breakup Required	Yes

ईएमडी विवरण/EMD Detail

एडवाईजरी बैंक/Advisory Bank	State Bank of India
ईएमडी राशि/EMD Amount	10000000

ईपीबीजी विवरण /ePBG Detail

एडवाइजरी बैंक/Advisory Bank	State Bank of India
ईपीबीजी प्रतिशत (%)/ePBG Percentage(%)	3.00
ईपीबीजी की आवश्यक अवधि (माह) /Duration of ePBG required (Months).	74

(a). जेम की शर्तों के अनुसार ईएमडी छूट के इच्छुक बिडर को संबंधित केटेगरी के लिए बिड के साथ वैध समर्थित दस्तावेज़ प्रस्तुत करने है। एमएसई

केटेगरी के अंतर्गत केवल वस्तुओं के लिए विनिर्माता तथा सेवाओं के लिए सेवा प्रदाता ईएमडी से छूट के पात्र हैं। व्यापारियों को इस नीति के दायरे से बाहर रखा गया है।/EMD EXEMPTION: The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD. Traders are excluded from the purview of this Policy.

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

लाभार्थी /Beneficiary :

PAO DCPW
PAO DCPW, CGO Complex, New Delhi
(Ao)

बोली विभाजन लागू नहीं किया गया/Bid splitting not applied.

एमआईआई अनुपालन/MII Compliance

एमआईआई अनुपालन/MII Compliance	Yes

1. If the bidder is a Micro or Small Enterprise as per latest orders issued by Ministry of MSME, the bidder shall be relaxed from the eligibility criteria of "Experience Criteria" as defined above subject to meeting of quality and technical specifications. The bidder seeking Relaxation from Experience Criteria, shall upload the supporting documents to prove his eligibility for Relaxation.
2. If the bidder is a Micro or Small Enterprise (MSE) as per latest orders issued by Ministry of MSME, the bidder shall be relaxed from the eligibility criteria of "Bidder Turnover" as defined above subject to meeting of quality and technical specifications. If the bidder itself is MSE OEM of the offered products, it would be relaxed from the "OEM Average Turnover" criteria also subject to meeting of quality and technical specifications. The bidder seeking Relaxation from Turnover, shall upload the supporting documents to prove his eligibility for Relaxation.
3. If the bidder is a DPIIT registered Startup, the bidder shall be relaxed from the the eligibility criteria of "Experience Criteria" as defined above subject to their meeting of quality and technical specifications. The bidder seeking Relaxation from Experience Criteria, shall upload the supporting documents to prove his eligibility for Relaxation.
4. If the bidder is a DPIIT registered Startup, the bidder shall be relaxed from the the eligibility criteria of "Bidder Turnover" as defined above subject to their meeting of quality and technical specifications. If the bidder is DPIIT Registered OEM of the offered products, it would be relaxed from the "OEM Average Turnover" criteria also subject to meeting of quality and technical specifications. The bidder seeking Relaxation from Turnover shall upload the supporting documents to prove his eligibility for Relaxation.
5. The minimum average annual financial turnover of the bidder during the last three years, ending on 31st March of the previous financial year, should be as indicated above in the bid document. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution / incorporation of the bidder is less than 3-year-old, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criteria.
6. Years of Past Experience required: The bidder must have experience for number of years as indicated above in bid document (ending month of March prior to the bid opening) of providing similar type of services to any Central / State Govt Organization / PSU. Copies of relevant contracts / orders to be uploaded along with bid in support of having provided services during each of the Financial year.
7. Estimated Bid Value indicated above is being declared solely for the purpose of guidance on EMD amount and for determining the Eligibility Criteria related to Turn Over, Past Performance and Project / Past Experience etc. This has no relevance or bearing on the price to be quoted by the bidders and is also not going to have any impact on bid participation. Also this is not going to be used as a criteria in determining reasonableness of quoted prices which would be determined by the buyer based on its own assessment of reasonableness and based on competitive prices received in Bid / RA process.
8. Past Experience of Similar Services: The bidder must have successfully executed/completed similar Services over the last three years i.e. the current financial year and the last three financial years(ending month of March prior to the bid opening): -
1. Three similar completed services costing not less than the amount equal to 40% (forty percent) of the estimated cost; or
2. Two similar completed services costing not less than the amount equal to 50% (fifty percent) of the estimated

cost; or
3. One similar completed service costing not less than the amount equal to 80% (eighty percent) of the estimated cost.

अतिरिक्त योग्यता /आवश्यक डेटा/Additional Qualification/Data Required

Scope of Work:1773645875.pdf

Payment Terms:1773645881.pdf

This Bid is based on Quality & Cost Based Selection (QCBS) . The technical qualification parameters are :-

Parameter Name	Max Marks	Cutoff Marks	Qualification Methodology Document
Average Annual Turnover	10	5	View File
Manpower	10	5	View File
Certifications	15	7	View File
Project Experience	25	13	View File
Technical Presentation	40	20	View File

Total Minimum Qualifying Marks for Technical Score: 50

QCBS Weightage(Technical:Financial):70:30

Presentation Venue: National Crime Records Bureau
NH 48, Service Lane
Mahipalpur
New Delhi 110037

Hiring Of Agency For IT Projects- Milestone Basis (1)

तकनीकी विशिष्टियाँ /Technical Specifications

विवरण/ Specification	मूल्य/ Values
कोर / Core	
Scope of Work	As specified in Scope of work
Resources Needed	As specified in Scope of work
Deployment of core team	hybrid(Buyer to specify model in scope of work)
Deliverables / Timelines	As specified in Scope of work
एडऑन /Addon(s)	

अतिरिक्त विशिष्टि दस्तावेज़ /Additional Specification Documents

---

परेषिती/रिपोर्टिंग अधिकारी /Consignees/Reporting Officer and Quantity

क्र.सं./S.No.	परेषिती/रिपोर्टिंग अधिकारी /Consignee Reporting/Officer	पता/Address	Quantity	अतिरिक्त आवश्यकता /Additional Requirement
1	Syed Ali Mahdi Rizvi	110037,National Crime Records Bureau, NH-8, Mahipalpur, New Delhi	Project / Lumpsum Based	N/A

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

1. **Generic**

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

2. **Generic**

   Actual delivery (and Installation & Commissioning (if covered in scope of supply)) is to be done at following address

   National Crime Records Bureau
   NH 48
   Service Lane
   Mahipalpur
   New Delhi 110037
   .

3. **Generic**

   Bidder financial standing: The bidder should not be under liquidation, court receivership or similar proceedings, should not be bankrupt. Bidder to upload undertaking to this effect with bid.

4. **Generic**

   Malicious Code Certificate:

   The seller should upload following certificate in the bid:-
   (a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code 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 will 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.

5. **Generic**

   1. The Seller shall not assign the Contract in whole or part without obtaining the prior written consent of buyer.
   2. The Seller shall not sub-contract the Contract in whole or part to any entity without obtaining the prior written consent of buyer.
   3. The Seller shall, notwithstanding the consent and assignment/sub-contract, remain jointly and severally liable and responsible to buyer together with the assignee/ sub-contractor, for and in respect of the due performance of the Contract and the Sellers obligations there under.

6. **Purchase Preference (Centre)**

   Purchase preference to Micro and Small Enterprises (MSEs): Purchase preference will be given to MSEs as defined in Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry of Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. If the bidder wants to avail the Purchase preference, the bidder must be the manufacturer of the offered product in case of bid for supply of goods. Traders are excluded from the purview of Public Procurement Policy for Micro and Small Enterprises. In respect of bid for Services, the bidder must be the Service provider of the offered Service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered product or service. If L-1 is not an MSE and MSE Seller (s) has/have quoted price within L-1+ 15% of margin of purchase preference /price band defined in relevant policy, such Seller shall be given opportunity to match L-1 price and contract will be awarded for percentage of 100% of total value.

7. **Service & Support**

   AVAILABILITY OF OFFICE OF SERVICE PROVIDER: An office of the Service Provider must be located in the state of Consignee. DOCUMENTARY EVIDENCE TO BE SUBMITTED.

8. **Service & Support**

   Dedicated /toll Free Telephone No. for Service Support : BIDDER/OEM must have Dedicated/toll Free Telephone No. for Service Support.

9. **Service & Support**

   Escalation Matrix For Service Support : Bidder/OEM must provide Escalation Matrix of Telephone Numbers for Service Support.

10. **Certificates**

    Bidder's offer is liable to be rejected if they don't upload any of the certificates / documents sought in the Bid document, ATC and Corrigendum if any.

11. **Payment**

    PAYMENT OF SALARIES AND WAGES: Service Provider is required to pay Salaries / wages of contracted staff deployed at buyer location first i.e. on their own and then claim payment from Buyer alongwith all statutory documents like, PF, ESIC etc. as well as the bank statement of payment done to staff.

12. **Past Project Experience**

    Proof for Past Experience and Project Experience clause: For fulfilling the experience criteria any one of the following documents may be considered as valid proof for meeting the experience criteria:a. Contract copy along with Invoice(s) with self-certification by the bidder that service/supplies against the invoices have been executed.b. Execution certificate by client with contract value.c. Any other document in support of contract execution like Third Party Inspection release note, etc.Proof for Past Experience and Project Experience clause: For fulfilling the experience criteria any one of the following documents may be considered as valid proof for meeting the experience criteria:a. Contract copy along with Invoice(s) with self-certification by the bidder that service/supplies against the invoices have been executed.b. Execution certificate by client with contract value.c. Any other document in support of contract execution like Third Party Inspection release note, etc.

13. **Forms of EMD and PBG**

    Bidders can also submit the EMD with Account Payee Demand Draft in favour of

    AO
    payable at
    PAO DCPW CGO Complex New Delhi
    .
    Bidder has to upload scanned copy / proof of the DD along with bid and has to ensure delivery of hardcopy

to the Buyer within 5 days of Bid End date / Bid Opening date.

14. **Forms of EMD and PBG**

Bidders can also submit the EMD with Fixed Deposit Receipt made out or pledged in the name of A/C

AO, PAO DCPW CGO Complex New Delhi
. The bank should certify on it that the deposit can be withdrawn only on the demand or with the sanction of the pledgee. For release of EMD, the FDR will be released in the favour of the bidder by the Buyer after making endorsement on the back of the FDR duly signed and stamped along with covering letter. Bidder has to upload scanned copy/ proof of the FDR along with bid and has to ensure delivery of hardcopy to the Buyer within 5 days of Bid End date/ Bid Opening date

15. **Forms of EMD and PBG**

Bidders can also submit the EMD with Banker’s Cheque in favour of

AO
payable at
PAO DCPW CGO Complex New Delhi
.
Bidder has to upload scanned copy / proof of the BC along with bid and has to ensure delivery of hardcopy to the Buyer within 5 days of Bid End date / Bid Opening date.

16. **Forms of EMD and PBG**

Successful Bidder can submit the Performance Security in the form of Account Payee Demand Draft also (besides PBG which is allowed as per GeM GTC). DD should be made in favour of

AO
payable at
PAO DCPW CGO Complex New Delhi
. After award of contract, Successful Bidder can upload scanned copy of the DD in place of PBG and has to ensure delivery of hard copy to the original DD to the Buyer within 15 days of award of contract.

17. **Forms of EMD and PBG**

Successful Bidder can submit the Performance Security in the form of Fixed Deposit Receipt also (besides PBG which is allowed as per GeM GTC). FDR should be made out or pledged in the name of

AO, PAO DCPW CGO Complex New Delhi
A/C (Name of the Seller). The bank should certify on it that the deposit can be withdrawn only on the demand or with the sanction of the pledgee. For release of Security Deposit, the FDR will be released in favour of bidder by the Buyer after making endorsement on the back of the FDR duly signed and stamped along with covering letter. Successful Bidder has to upload scanned copy of the FDR document in place of PBG and has to ensure delivery of hard copy of Original FDR to the Buyer within 15 days of award of contract.

18. **Buyer Added Bid Specific ATC**

Buyer Added text based ATC clauses

Bidder has to provide following declaration on Company's Letterhead

DECLARATION BY THE BIDDER

1. We do not have any criminal proceedings against us.

2. We have not been blacklisted / terminated / debarred by any Central Government Ministry/ Department/ Organization. Document to be submitted on Bidder’s Letter Head

3. If we are entrusted with the work, we assure you that we will undertake the required work properly for t he full tenure as quoted, failing which we will be liable for blacklisting and other punitive action by NCRB. New Delhi.

4. We have read, understood and accept all the terms and conditions of the tender.

5. We hereby certify that the information furnished by us is true and correct to the best of our knowledge. We understand that in case if any of the information/details furnished by us is found to be false or incorrec t at any stage or if our company indulges in malpractices of any kind, our company will be liable for being blacklisted for future transaction with the Department.

6. We are not bankrupt, under liquidation, court receivership or similar proceedings. Document to be subm itted on Bidder's Letter Head.

.

19. **Buyer Added Bid Specific ATC**

    Buyer uploaded ATC document Click here to view the file.

अस्वीकरण/Disclaimer

The Additional Terms and Conditions (ATC) have been incorporated by the Buyer after approval of their Competent Authority. The Buyer ,is solely responsible for the impact of these clauses on the bidding process, its outcome, and consequences thereof including any restriction arising in the bidding process due to these ATCs and including the modification of technical specifications and / or terms and conditions governing the bid.All representations / grievances pertaining to the ATC clauses shall be raised with the buyer organization directly and not with GeM.If any of the clause(s) is/are incorporated by the Buyer regarding the following, the bid & resultant contract shall be treated as null & void. Further, GeM reserves the right, at its sole discretion, to cancel the bid forthwith, without issuance of any prior notice or intimation :-

1. Publishing Custom / BOQ bids for items for which regular GeM categories are available (unless such Custom / BOQ item is bunched with the major regular product Category Item).
2. Mandating procurement of / from specific Brand / Make / Model / Manufacturer / Dealer except in case of Single Bid / Proprietary Article Certificate (PAC) Buying.
3. Inclusion of disqualification criteria related to suspension of seller / service provider, where such suspension period has already expired.
4. Mandating submission of documents in physical form as a pre-requisite to qualify bidders.
5. Publishing bids on GeM for procurement of works.
6. Procurement of Goods by creating a Service bid on GeM & vice-versa.
7. Seeking sample with bid or approval of samples during bid evaluation process. However, trial / sample, as the case may be, shall be permitted in cases where trial / sample are allowed as per approved and published procurement policy of the Buyers' controlling Ministry / Department / State / Public Sector Enterprises Headquarters. If there is any violation of trial / sample clause with regard to approved policy of the Buyers' Ministry / Department / State / Public Sector Enterprises Headquarters, then this is to be determined and redressed by the concerned Buyer Organisation only.
8. Seeking experience from specific organization / department / institute only or from foreign / export experience.
9. Creating bid for items from incorrect categories.
10. Reference of conditions published on any external site or reference to external documents/clauses.
11. Asking for any Tender fee / Bid Participation fee, as the case may be.
12. Buyer added ATC Clauses which are in contravention of clauses defined in bid detail section, including specifications, EMD Detail, ePBG Detail and MII and MSE Purchase Preference sections of the bid, unless otherwise allowed by the applicable GeM GTC.
13. Any ATC clause in contravention with GeM GTC Clause 4 (xiii) (h) will be invalid. In case of multiple L1 bidders against a service bid, the buyer shall place the Contract by selection of a bidder amongst the L-1 bidders through a Random Algorithm executed by GeM system.
14. In a category based bid, adding additional items, through buyer added, additional scope of work/ additional terms and conditions/or any other document. If buyer needs more items along with the main item, the same must be added through bunching category based items or by bunching custom catalogues or bunching a BoQ with the main category based item, the same must not be done through ATC or Scope of Work.

Further, if any seller has any objection/grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in

the bid details field in Seller dashboard after logging in as a seller. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations.

All GeM Sellers/Service Providers shall ensure full compliance with all applicable labour laws, including the provisions, rules, schemes and guidelines under the four Labour Codes i.e. the Code on Wages, 2019; the Industrial Relations Code, 2020; the Occupational Safety, Health and Working Conditions Code, 2020; and the Code on Social Security, 2020 as and when notified and brought into force by the Government of India.

For all provisions of the Labour Codes that are pending operationalisation through rules, schemes or notifications, the corresponding provisions of the pre-existing labour enactments (such as The Minimum Wages Act, 1948, The Payment of Wages Act, 1936, The Payment of Bonus Act, 1965, The Equal Remuneration Act, 1976, The Payment of Gratuity Act, 1972, etc. and relevant State Rules) shall continue to remain applicable.

The Seller/ Service Providers shall, therefore, be responsible for ensuring compliance under:

- **All notified and enforceable provisions of the new Labour Codes as mentioned hereinabove; and**
- **All operative provisions of the erstwhile Labour Laws until their complete substitution.**

All obligations relating to wages, social security, safety, working conditions, industrial relations etc. and any other statutory requirements shall be strictly met by the Seller/ Service Provider. Any non-compliance shall constitute a breach of the contract and shall entitle the Buyer to take appropriate action in accordance with the contract and applicable law.

This Bid is governed by the General Terms and Conditions, conditions stipulated in Bid and Service Level Agreement specific to the Service, as the case may be, as provided in the Marketplace.

However, in case of Service, if any condition specified in General Terms and Conditions is contradicted by the conditions stipulated in Service Level Agreement specific to said Service, then it will over-ride the conditions in the General Terms and Conditions.

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

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

---धन्यवाद/Thank You---