Haryana Power Generation Corporation Limited
(A Government of Haryana Undertaking)
Urja Bhawan,
Sector-6, Panchkula
Haryana-134109

HPGCL

E-TENDER NIT

FOR

Supply, installation & commissioning of Cyber Security Solution including hardware, comprehensive warranty, licenses and premium support and onsite engineer for a period of 5 years

Ref No. Ch-48/IT/GNL-17/Vol-II dated 24 /02/2026

Bid Submission end date 27/03/26 **(by 15.00 Hrs)**

Table of Contents

1. DEFINITIONS.

For the purpose of this document, the expressions mentioned hereunder shall have the meaning specified against them unless there is anything repugnant in the subject or context:

(a)	**'Owner' or 'Employer'**	Shall mean the Haryana Power Generation Corporation Limited (HPGCL), a Company incorporated under the Companies Act, 1956 having its registered office at Urja Bhawan, C-7, Sector-6, Panchkula, Haryana and its power stations, units and all offices under its control.
(b)	**'Tender'**	Shall mean the tender submitted by the tenderer for acceptance by the Owner.
(c)	**'Managing Director'**	Shall mean the Managing Director (MD) of HPGCL, or his successors in office as designated by the Owner.
(d)	**'Agency' or 'Contractor'**	Shall mean the person or persons, firm or company whose tender has been accepted by HPGCL and includes the Contractor's legal representatives, his successors and permitted assignees.
(e)	**'Sub-contractor'**	Shall mean any person or firm or company (other than the contractor) to whom any part of the work has been entrusted by the Contractor, with the written consent of the owner or his representative and the legal representatives, successors and permitted assignee of such person, firm or company.
(f)	**'Contract'**	Shall mean the agreement between the Owner and the agency for execution of the contract including therein all documents such as the invitation to Tender, instructions to tenderer, Special Conditions of Contract, Scope of Work, agreed Variations if any etc.
(g)	**'Contract Document'**	Shall mean collectively the tender documents, agreed variations, if any and other documents

		constituting the tender and acceptance thereof.
(h)	**'Site'**	Shall mean the locations and places wherever business activities are conducted by the Owner. A list of such locations is provided at clause no. 6.1.
(i)	**'Plant'**	Shall mean the Power Generating station of HPGCL.
(j)	**'Offices'**	Shall mean Corporate Office and Offices at various Power Generating station of HPGCL
(k)	**'Notice'**	Shall mean a notice in written, typed or printed characters sent (unless delivered personally or otherwise proved to have been received) by registered post/speed post/e-mail to the last known private or business address or registered office of the addressee and shall be deemed to have been received in the ordinary course of post/electronic post it would have been delivered.
(l)	**'Appointing Authority'**	Shall be the Managing Director or any other person so designated by him for the purpose of arbitration.
(m)	**'Letter of Award'**	Shall mean intimation by a Letter to tenderer that the tender has been accepted in accordance with the provisions contained in the letter.
(n)	**'Days'**	Shall mean a calendar day of 24 hours from midnight to midnight irrespective of the number of hours worked in that day.
(o)	**Total Value of Contract'**	Shall mean the total bid price including all applicable taxes in accordance with the prices accepted in tender as payable to the agency for providing the consulting services
(p)	**'PTPS Panipat'**	Shall include both PTPS-1 and PTPS-2 Panipat.

In the event of any doubts arising with respect to the provisions of the rules and inadequacy in the scope of its coverage, the final authority of interpretation shall vest with the MD whose decision shall be final.

2. INTRODUCTION

Haryana Power Generation Corporation Ltd. came into existence on 14.08.98 after the restructuring of Haryana State Electricity Board into Haryana Power Generation Corporation Ltd. (HPGCL), Haryana Vidyut Prasaran Nigam Ltd. (HVPNL), Uttar Haryana Bijli Vidyut Nigam Ltd.(UHBVNL) & Dakshin Haryana Bijli Vidyut Nigam Ltd. (DHBVNL) under the Reform Programme.

The main objectives of HPGCL are as under: -

a) To generate power from its existing Generating Stations in the most efficient manner on commercial lines and to sell the same to distribution companies.

b) To set up new Power Generation Projects.

HPGCL owns & operates the following power plants in the state:

Sr.No	Name of Power Station	Unit Details	Total Capacity (MW)
i.	Panipat Thermal Power Station.	1x210MW+2x250MW	710 MW
ii.	Deen Bandhu Chhotu Ram Thermal Power Project(DCRTPP), Yamuna Nagar.	2x300 MW	600 MW
iii.	Rajiv Gandhi Thermal Power Project(RGTPP), Khedar, Hisar	2x600 MW	1200 MW
iv.	WYC Hydro Electric Station, Yamuna Nagar	6x8MW+2x7.2MW	62.4 MW
v.	Solar Power Plant at PTPS, Panipat	10 MW	10 MW

3. SECTION I: INSTRUCTION TO BIDDERS

3.1. e-TenderingProcess

3.1.1. e-Tendering Portal

Bidders can download tender documents from the portal: https://etenders.hry.nic.in. Bidders shall have to pay Tender document fee, e-Service fee and EMD online by using the service of secure electronic payment gateway. The secure electronic payment gateway is an online interface between bidders / contractors and online payment authorization networks. Payment for Tender Document Fee and e-Service Fee can be made by bidders / contractors online directly through Debit Cards / Internet Banking Accounts / any other online mode and payment for EMD can be made online directly through RTGS / NEFT/ any other online mode.

NOTE: If tender is cancelled or recalled on any ground, the tender document fee & e-service fee will not be refunded to the bidders.

3.1.2. Registration of Bidders on e-Procurement Portal

All the bidders intending to participate in the tenders processed online are required to get registered on the centralized e-Procurement Portal i.e. https://etenders.hry.nic.in. Please visit the website for more details.

3.1.3. Obtaining a Digital Certificate

1) The Bids submitted online should be encrypted and signed electronically with a Digital Certificate to establish the identity of the bidder bidding online. These Digital Certificates are issued by an Approved Certifying Authority, by the Controller of Certifying Authorities, Government of India.
2) The bidders may obtain Class-III digital signature certificate from any Certifying Authority or Sub-certifying Authority authorized by the Controller of Certifying Authorities.
3) Bid for a particular tender must be submitted online using the digital certificate (Encryption & Signing), which is used to encrypt the data and sign the hash during the stage of bid preparation & hash submission. In case, during the process of a particular tender, the user loses his digital certificate (due to virus attack, hardware problem, operating system or any other problem) he will not be able to submit the bid online. Hence, the users are advised to keep a backup of the certificate and also keep the copies at safe place under proper security (for its use in case of emergencies).
4) In case of online tendering, if the digital certificate issued to the authorized user of a firm is used for signing and submitting a bid, it will be considered equivalent to a

no-objection certificate/power of attorney /lawful authorization to that User. The firm has to authorize a specific individual through an authorization certificate signed by all partners to use the digital certificate as per Indian Information Technology Act 2000. Unless the certificates are revoked, it will be assumed to represent adequate authority of the user to bid on behalf of the firm in the department tenders as per Information Technology Act 2000. The digital signature of this authorized user will be binding on the firm.

5) In case of any change in the authorization, it shall be the responsibility of management / partners of the firm to inform the certifying authority about the change and to obtain the digital signatures of the new person / user on behalf of the firm / company. The procedure for application of a digital certificate however will remain the same for the new user.
6) The same procedure holds true for the authorized users in a private/Public limited company. In this case, the authorization certificate will have to be signed by the directors of the company.

3.1.4. Electronic Payment.

Tender document can be downloaded online. Bidders are required to pay the tender documents fees online using the electronic payments gateway service. For online payments guidelines, please refer to the Home page of the e-tendering Portal https://etenders.hry.nic.in.

3.1.5. Pre-requisites for online bidding

In order to bid online on the portal https://etenders.hry.nic.in, the user machine must be installed with Java as per requirement of e-tendering Portal.

3.1.6. Online Viewing of Detailed Notice Inviting Tenders

The bidders can view the detailed NIT and the time schedule (Key Dates) for all the tenders floated through the single portal e-Procurement system on the Home Page at https://etenders.hry.nic.in.

3.1.7. Key Dates

The bidders are strictly advised to follow dates and times as indicated in the Bid Data Sheet. The date and time shall be binding on all bidders. All online activities are time tracked and the system enforces time locks that ensure that no activity or transaction can take place outside the start and end dates and the time of the stage as defined in the online Notice Inviting Tenders.

3.1.8. Mode of Payment for submission of tender

3.1.7.1 The online payment for Tender document fee, eService Fee & EMD can be done using the secure electronic payment gateway. The Payment for Tender Document Fee and eService Fee can be made by eligible bidders/ contractors online. The transaction reference no. will be intimated to HPGCL along with supported documents.

3.1.7.2 The secure electronic payments gateway is an online interface between contractors and online payment authorization networks.

3.1.7.3 Please visit HPGCL website www.hpgcl.org.in and https://etenders.hry.nic.in for NIT details.

3.1.7.4 Bidders are instructed to submit their bids online only on Haryana e-portal website (https://etenders.hry.nic.in).

3.1.7.5 Unless exempted specifically, tenders not accompanied with the prescribed EMD/Cost of Tender shall be rejected. EMD/Cost of Tender shall be in the prescribed mode of payment as asked in the NIT, otherwise the tender shall be liable to be rejected.

3.1.7.6 Tender received through Telefax / email or in physical form shall not be considered.

3.1.7.7 In case, date specified for opening of tender, happens to be a public holiday, then next working day shall be considered automatically for the same.

3.1.7.8 All the costs and expenses incidental to the preparation of tender, discussions, conferences, if any, shall be borne by the tenderers and HPGCL shall bear no liability whatsoever on such costs and expenses.

3.2. Date of Validity

The validity of tender shall be 120 days from the date of opening of Part-II 'Price Bid'. It is the responsibility of the Bidders to ensure that Bids are delivered in accordance with the instructions set out in the NIT and its accompanying documents.

3.3. Preparation of Bids

3.3.1. Language of Bid

1) The Bid, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Purchaser, shall be written in the English. Supporting documents and printed literature that are part of the Bid may be in another language provided they are accompanied by an accurate translation of the

relevant passages in English, in which case, for purposes of interpretation of the Bid, such translation shall govern.

3.3.2. Documents comprising the Bid

1) The Bid shall comprise following details:

   a) (i) Earnest Money Deposit and (ii) Proof of Purchasing Tender document, e-Service Fee as per BDS (Bid Data Sheet).

   b) Relevant documents related to "Technical Proposal"

   c) Relevant formats / details related to "Price Proposal"

3.3.3. Earnest Money Deposit (EMD) and Security Deposit

Earnest Money Deposit (EMD)

1) The Bidders shall have to pay for EMD Fees online through e-Tendering portal. The bidder shall also be required to pay for Tender documents Fee & e-Service Fee online by using the service of secure electronic payment gateway as per details mentioned in the BDS.
2) The EMD of the unsuccessful bidder will be returned without any interest within 30 days after award of contract to successful bidder. The Earnest Money Deposit of the successful bidder shall be adjusted into the security deposit from 1st invoice as a guarantee for faithful and satisfactory execution of the work.

Security Deposit:

The Security Deposit shall be 2% of the Part-A of the Contract value and shall be 10% of the Part-B of the Contract value for faithful execution of the contract. The EMD already deposited by successful bidder shall be converted into the security deposit of Part–A and balance amount if any shall be deducted from the first invoice. For security deposit of Part -B, an amount equivalent to 10% of the Payments/Quarterly running bills shall be deducted and kept as security deposit.

Release of Security deposit:

3) PART-A: The EMD of the successful tenderers on whom the work order is placed will be converted into security deposit which shall be released 30 days after completion of the contract period of 5 years post installation & commissioning.
4) Part-B: The Security Deposit deducted as the 10% amount shall be released 30 days after completion ofthe contract period of 5 years post installation & commissioning.
5) No interest shall be paid on EMD/ Security Deposit for the period it remains deposited with HPGCL.
6) The earnest money /security deposit shall be forfeited in part or in full under the following circumstances:
   a. If the tenderer withdraws his tender at any stage during the currency of his validity period.
   b. If the order has been issued but the tenderer refuses to comply with it.
   c. Where the order has been complied with but the supplier stops making the supplies/commissioning after partially fulfilling the order.
   d. In the event of breach of a contract in any manner.

e. In the case of evidence of cartel formation by the bidder(s).
f. In case the bidder has submitted or submits false / forged information or documents.

3.3.4. Price Schedules

1) The Bidders should take note of following points while submitting the Price Proposal:
   a) Price Proposal should clearly indicate the price to be charged without any qualifications whatsoever and should include all taxes, duties as may be applicable, to be paid pre- or post-delivery or to be deducted by the purchaser at source, in relation to the Goods and Related Services.
   b) If price for any Good, Component or Services as required in the Price Proposal is not quoted, it will be considered as included in the price proposal. No addition or modification to the quoted price will be allowed.
2) All items in the Schedule of Supply must be listed and priced separately in the Price Schedules. If an item listed in Price Schedule is not priced, the bidder shall notify specifically that the price of said item is included in the prices of other items and also specifying their Sr.No.
3) Prices quoted by the Bidder must be firm and final and shall remain constant throughout the period of the contract and shall not be subject to any upward revision.

3.3.5. Currency of Bid

1) Bidders may express their bid price in Indian Rupees only.

3.4. Submission of Bids

1) Bids shall be of two part: (a) Technical Bid, and (b) Financial Bid
2) The bidders shall upload their technical offer containing documents, qualifying criteria, technical specification, schedule of deliveries, and all other terms and conditions except the rates (price bid).
3) The bidders shall quote the prices in price bid format only.
4) Submission of bids will be preceded by submission of the digitally signed & sealed bid (Hash) as stated in the time schedule (Key Dates) of the Tender.
   a. If bidder fails to complete the Online Bid Submission stage on the stipulated date and time, His/hers bid will be considered as bid not submitted, and hence not appear during tender opening stage.
   b. Bidders participating in online tenders shall check the validity of his/her Digital Signature Certificate before participating in the online Tenders at the portal https://etenders.hry.nic.in
   c. For help manual please refer to the 'Home Page' of the e-Procurement website at https://etenders.hry.nic.in.
5) HPGCL reserves the right to select or reject any party without assigning any reason whatsoever.

3.4.1. Technical Bids

1) The Bidder is expected to examine all terms and conditions included in the Document. Failure to provide the requested information will be at his risk

and may result in rejection of the Bid.

2) Technical Bid must provide the information, using, but not limited to, the formats attached as annexure in bid.
3) Technical Bids needs to include Bidder's understanding of the processes, the proposed solution including an elaboration of how the required tasks are proposed to be undertaken
4) TECHNICAL BID MUST NOT INCLUDE ANY FINANCIAL INFORMATION. IF FOUND SO THE BIDDER WILL BE DISQUALIFIED.

3.4.2. Financial Bids

The financial Bid must take into account the tax liability & cost of insurances if any and any other statutory pay-outs as per the standard guidelines.

3.4.3. Late Bids

The Purchaser shall not consider any Bid that arrives after the deadline for submission of Bids. Any Bid received by the Purchaser after the deadline for submission of Bids shall be declared late; rejected, and returned unopened to the Bidder.

3.4.4. Withdrawal, Substitution and modification of bids

A Bidder may not withdraw, substitute, or modify its Bid after due date of bid submission.

3.5. Evaluation and Comparison of Bids

3.5.1. Responsiveness of Technical Proposal

1) The Purchaser's determination of the responsiveness of a Technical Proposal will be based on the contents of the Technical Proposal itself.
2) A substantially responsive Technical Proposal is one that conforms to all the terms, conditions, and specifications of the Bidding Document including all required forms, documents, compliances as defined in the bid document without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that:
   a) affects in any substantial way the scope, quality, or performance of the Goods and Related Services specified in the Contract; or
   b) limits or is inconsistent in any substantial way, with the Bidding Document, the Purchaser's rights or the Bidder's obligations under the Contract; or
   c) if rectified would unfairly affect the competitive position of other Bidders presenting substantially responsive Technical Proposals.
3) If a Technical Proposal is not substantially responsive to the Bidding Document, it shall be rejected by the Purchaser and shall not subsequently be made responsive by the Bidder by correction of the material deviation, reservation, or omission.

3.5.2. Non conformities, Errors, and Omissions

1) Provided that a Technical Proposal is substantially responsive, the Purchaser may waive any nonconformity or omission in the Bid that does not constitute a material deviation.
2) Provided that a Technical Proposal is substantially responsive, the Purchaser may request that the Bidder submit the necessary information or documentation, within a reasonable period of time, to rectify non-material non-conformities or omissions in the Technical Proposal related to documentation requirements. Such omission shall not be related to any aspect of the Price Proposal of the Bid. Failure of the Bidder to comply with the request may result in the rejection of its Bid.
3) Provided that the Technical Proposal is substantially responsive, the Purchaser will correct arithmetical errors during evaluation of Price Proposals on the following basis:
   a) if there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected, unless in the opinion of the Purchaser there is an obvious misplacement of the decimal point in the unit price, in which case the total price as quoted shall govern and the unit price shall be corrected;
   b) if there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected;
   c) if there is a discrepancy between words and figures, the amount in words shall prevail. However, where the amount expressed in words is related to an arithmetic error, the amount in figures shall prevail subject to (a) and (b) above;
   d) if there is a discrepancy between percentage and figures related to various taxes or levies, the percentage shall prevail over figure mentioned. However, where the amount expressed in percentage is related to an arithmetic error, the amount in figures shall prevail subject to (a) and (b) above. It should also be noted that at time of payment against, the prevailing tax/levy rates will be used as on the date of approval of payment.
4) Except as provided in sub-Clauses (a) to (d) herein above, the Purchaser shall reject the Price Proposal if the same contains any other computational or arithmetic discrepancy or error.
5) If the Bidder that submitted the lowest evaluated Bid does not accept the correction of errors, its Bid shall be disqualified and its Earnest Money Deposit shall be forfeited.

3.5.3. Examination of Terms & Conditions

1) The Purchaser shall examine the Bids to confirm that all terms and conditions specified in the GCC and the SCC have been accepted by the Bidder without any material deviation or reservation.
2) The Purchaser shall evaluate the technical aspects of the submitted Bid to confirm that all requirements specified in the Section IV: Scope of Work, of the Bidding Document have been met without any material deviation or

reservation.

3) If, after the examination of the terms and conditions, the Purchaser determines that the Technical Proposal is not substantially responsive in accordance with Clause 3.5.1, it shall reject the Bid.

4) The Purchaser reserves the right to verify the credentials (including documents, declarations, self-certifications etc.) provided by the Bidders by its own means and methods. In case Purchaser receives feedback contrary to the responses of the Bidder or is not satisfied with compatibility of the experience with the required standards / expectations, Purchaser reserves the right to form its own opinion and even reject the bids.

3.5.4. Deviations

Deviations, if taken by the bidder(s) on the specifications, terms & conditions of the tender documents will not be acceptable. No deviations certificate should be attached as per**Annexure-4**.

3.5.5. Evaluation of Price Bids

1) The Purchaser shall evaluate Price Proposals of each Bid for which the Technical Proposal has been determined to be substantially responsive.

2) To evaluate a Technical Proposal, the Purchaser shall only use all the criteria and methodologies defined in NIT and any other approach specified in the bid document.

3) To evaluate a Price Proposal, the Purchaser shall consider the Bid Price quoted in Price Proposal Submission Sheet i.e. inclusive of all duties, levies and taxes.

3.5.6. Comparison of Bids

1) Total Contract Value (TCV) will be calculated based on response provided in the price proposal. Price Bid evaluation will be done on total prices all inclusive of taxes, duties and levies.

2) The TCV of the Bidder will be calculated on the basis of Grand Total Cost defined in Section-VII Price bid schedule.

3) The Bid having the Lowest TCV shall be termed as the Lowest Evaluated Bidder.

3.6. Purchaser's Right accept or reject any or all bids

The Purchaser reserves the right to accept or reject any or all Bid, or annul the bidding process and reject any or all Bids at any time prior to Contract award without assigning any reasons and without thereby incurring any liability to the Bidders.

3.7. Award of Contract

3.7.1. Award Criteria

1) The final bidder will be selected on the basis of lowest price quoted under final schedule of requirement and price bid schedule i.e. Section-VII and contract will be awarded to the lowest bidder.

2) Negotiations:-

Negotiations, if required would be held by competent authority of HPGCL with reference to Haryana Govt. O/o no. 2/2/2010-4-IB-II dated 18.06.2013 & 2/2/2010-4-IB-II dated 16.06.2014 and its latest amendment dated order No 14/26/2023-6FA dated 10.05.2023.

a) Price negotiation could be held up to four number of such bidder (s), in addition to L1- bidder in cases where there are bidders falling within 5% of the L-1 bidder. In cases where the L-1 bidder refuses to further reduce his offered price and any of the four bidders come forward to offer a price which is better than the price offered by L-1 bidder, the bidder whose price is accepted becomes the L-1 bidder. However, in such a situation, the original L1 bidder may be given one more opportunity to improve upon the discovered price. In case, the original L1 bidder further improves upon the price discovered during the negotiations, he would be treated as the L1 bidder.

b) In cases where there is no bidder within 5% of the L-1 bidder,

i) L-2 bidder will be invariably called for negotiation in addition to the L-1 bidder and

ii) L-3 bidder will also be called, if it is so decided by the competent authority, in addition to L-1, L-2 bidders.

3) A Bid shall be rejected if the pre-qualification criteria specified in Section III are no longer met by the bidder whose offer has been determined to be the lowest evaluated Bid. In this event the purchaser shall proceed to the next lowest evaluated bid to make a similar reassessment of that bidder's capabilities to perform satisfactorily.

3.7.2. Letter of Award

1) Prior to the expiration of the period of bid validity, the Purchaser shall notify the successful Bidder, in writing, that its Bid has been accepted and will issue the Letter of Award (LoA)

2) Until a formal contract is prepared and executed, the notification of award or LoA shall constitute a binding contract.

3.7.3. Signing of Contract

The contractor shall execute a contract agreement with HPGCL on a Non Judicial Stamp Paper of appropriate value within 15 days of receipt of work order.

3.7.4. Period of Contract

The contract period shall include 150 days of supply, installation and commissioning and also includes 5 years of comprehensive Warranty of EDR, Anti-APT/Sandbox, Secure Access Service Edge (SASE), etc. post installation & commissioning and 5 years of onsite Resident Engineers deployment. In case of any delay, the contract period will extend accordingly.

3.7.5. Performance bank Guarantee

Within fifteen (15) days of the receipt of work order from the purchaser, the successful bidder shall furnish the performance bank guarantee. The same shall stand forfeited in case of cancellation of the contract for any breach of contract or for any deficiency in the performance noticed during the currency of the contract.

3.7.6. Note

1) If bidder fails to complete the Online Bid Submission stage on the stipulated date and time, his/her bid will be considered as bid not submitted, and hence will not appear during tender opening stage.
2) Bidders participating in online tenders shall check the validity of his/her Digital Signature Certificate before participating in the online tenders at the portal https://etenders.hry.nic.in. For help manual please refer to the 'Home Page' of the e-Procurement website at https://etenders.hry.nic.in and click on the available link 'Information about DSC'.
3) For help manual please refer to the 'Home Page' of the e-Procurement website at https://etenders.hry.nic.in and click on the available link 'Help to Contractor'.
4) For any technical related queries please call at 24 x 7 Help Desk Number given on the 'Home Page' of the e-Procurement website at https://etenders.hry.nic.in and click on the available link 'Contact Us'.
5) These conditions will over-rule the conditions stated in the tender documents, wherever relevant and applicable.

4. Section II: Bid Data Sheet

4.1. Bidding Document
The Purchaser's address is: O/o XEN/IT& ERP O/o CE/REO **Haryana Power Generation Company Limited**, Urja Bhawan, C-7, Sector-6, Panchkula, Haryana, India Phone/Fax: 91-172-5022416 Email: it@hpgcl.org.in
4.2. Preparation of Bids
The language of the Bid is: English
a) The e-Service fee shall be required and the amount required to be furnished is Rs. 1180/- (Rupees One Thousand one hundred Eighty only) b) The Tender Document Fee shall be required and the amount required to be furnished is Rs. 5900/- (Rupees Five Thousand Nine hundred only). c) The Earnest Money Deposit amounting to Rs. 25 Lakh (Rupees Twenty Five Lakh only) shall be required to be furnished online as per Clause No. 3.1 & 3.3.3.
Bidders can submit their tender documents (online) as per the following key dates:- **Start date and time** Date: 24.02.2026 Time: **17:00hrs (**IST)
The Pre-Bid meeting shall be held on:11.03.2026 at 11:00 hrs (IST) **Venue**: Haryana Power Generation Corporation Limited, Urja Bhawan C-7, Sector-6, Panchkula. **Bid related queries:** Bidders should note the following for bid related queries/ clarifications: 1. All queries / clarifications related to the bid document need to be emailed latest by 06.03.2026 (17.00hrs) 2. All queries /clarifications needs to be sent at it@hpgcl.org.in. No other email ID or mode of submission will be allowed. 3. Bidders needs to clearly mention (i) Page No., (ii) Clause No. and (iii) Query/Clarification required Bidders need to email MS Excel along with the PDF version of queries/clarifications. **NOTE**: Wherever reference to "Time" has been made, the same shall be taken as Indian Standard Time.
Bid Submission end date and time Date: 27.03.2026 Time: **15:00hrs (**IST)
The **Technical bid opening shall take place** online as per following schedule: Date: 30.03.2026 Time: **12:30 hrs (**IST)

5. Section III: Qualifying Criteria.

The Firm intending to bid should fulfill the following eligibility criteria (**satisfactory evidence to be provided by the firm**):

a) The tender is open to all firms/companies from within India, who are eligible to do business under relevant Indian laws as in force at the time of bidding.

b) Firm/company declared by GoI, GoH to be ineligible to participate for corrupt, fraudulent or any other unethical business practices shall not be eligible during the period for which such ineligibility is declared.

S. No	Basic Requirement	Specific Requirements	Documents Required
1.	Legal Entity	The bidder eligible for participating in the bidding process shall be a legal Business Entity.	- Copy of valid Registration Certificates - Copy of Certificates of incorporation
2.	Turnover	The bidder should have Minimum Average Annual Turnover of INR 4.98 Crore of last three financial years (i.e. year 2022-23, year 2023-24& year 2024-25). The net profit of the company shall be positive each of the last three financial years.	Audited Financial Statements With Certificate from statutory auditors clearly certifying the turnover requirements
3.	Experience	Bidder must have successfully executed one work of 19.93 Crore "or" two works of 12.46 Crore "or" three works of 9.96 Crore for similar Systems during last 5 financial years for similar work viz any kind of Cyber Infrastructure, Firewalls, Networking equipment's etc.	**Work orders** along with successful completion issued by purchaser department.
4.	Tax registration	The bidder should have a registered number of Income Tax / PAN number GSTIN	- Copy of PAN Card - Copy of valid GST certificate
5.	Mandatory Undertaking	The Bidder should not be debarred/blacklisted by any Government / PSU in India as on date of submission of bid.	Self Undertaking.

S. No	Basic Requirement	Specific Requirements	Documents Required
6.	OEM Authorization	The Bidder should have authorization from the Original Equipment Manufacturer (OEM) for the equipment's i.e.EDR, Anti-APT/Sandbox etc.	Manufacturer's Authorization Form to be submitted.
7.	OEM Technical Compliance	The Bidder shall submit technical compliance vetted by OEM for under Section 9 i.e Technical Specifications	Manufacturer's vetted compliance on their letterhead with stamp.

6. SECTION-IV: Scope of work

6.1.1. Objective

A Cyber security in an organization shall consist of a specialized set of People, Processes and Technology dedicated to monitoring and defending organizational IT assets, and detecting, containing, eradicating and assisting in the recovery from security threats and associated incidents.

The increasing digitization and connectivity of power generation plants have made them more efficient but also more vulnerable to cyber threats. Cyber security solutions are essential to protect the critical infrastructure of these plants from cyber attacks that could lead to operational disruptions, financial losses, and safety hazards.

Importance of Cyber Security in Power Generation Plants

- **Operational Continuity**: Ensuring continuous operation and minimizing downtime are crucial for maintaining the stability of the system.
- **Safety**: Cyber attacks can lead to hazardous situations, potentially endangering plant personnel and the public.
- **Regulatory Compliance**: Adhering to regulatory requirements and standards is necessary to avoid legal penalties and ensure the plant's operational legitimacy.

6.1.2. Scope Summary

In Power Sector a mature cyber security solution is required in running the operations efficiently. It is designed with objective to reduce the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) through automation and autonomous operations.

The key solution for an integrated security and automated response capabilities for providing the security from end point to network level has been designed keeping in view of the Govt of India and cert-in cybersecurity guidelines.

Key Solutions required for cyber security for HPGCL Network across HPGCL:

- EDR (Endpoint Detection & Response),
- Anti-APT(Sandbox),
- Secure Access Service Edge (SASE)

The combination of EDR, Sandbox, SASE offers a comprehensive security approach for power generation plants. Tailoring the security solution to the specific needs of the plant and continuously evaluating and updating the security posture are key to maintaining robust protection against evolving threats.

By implementing these key solutions, power generation networks can significantly enhance their cybersecurity posture, reduce MTTD and MTTR, and ensure compliance with CERT-IN guidelines.

Manpower Requirements

The Firm must deploy the Onsite Resident Engineers as per the Locations decided by HPGCL and must include the provision of following skilled personnel:

- Cyber security Manager: 1
- Cyber Security Engineers: 3

EDR (Endpoint Detection & Response)

EDR (Endpoint Detection & Response) delivers real-time, automated endpoint protection with orchestrated incident response across any protected device. This protection includes desktops/laptops, servers, and cloud workloads with current and legacy operating systems, as well as manufacturing and OT systems.

End point protection with latest capabilities like know attacks (Signature based), Zero day (APT/Zero day/unknown attacks protection at end point/User level with complied machines) is required which can be achieved with the help of end point protection tools like Zero trust Network protection, End point protection or EDR.

Pre-Infection Protection

Provides a proven first layer of defense via next-generation machine-learning-based antivirus (NGAV) engine that prevents infection from advanced attacks like ransomware.

Post-Infection Protection

EDR is the solution that detects and stops advanced attacks in real time, even when the endpoint has been compromised. No breaches, no data loss, no problem. EDR eliminates dwell time and provides a suite of automated endpoint detection and response (EDR) features to detect, defuse, investigate, respond to, and remediate incidents.

Empower the Cyber security

- Discover and control rogue devices (e.g., unprotected or unmanaged devices) and IoT
- devices.
- Track applications and ratings
- Discover and mitigate the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies.
- Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database.
- Protect disconnected endpoints with offline protection.

- Leverage application control to easily add allowed or blocked applications to pre-defined lists. This feature is useful for locking down sensitive systems like POS devices.
- USB device control.

Agent and Licensing

- Unified agent or logically integrated agent architecture
- Licensed for minimum 850 endpoints
- Signature-based and AI/ML-based detection

Protection Capabilities

- Anti-ransomware, anti-exploit, anti-bot and anti-malware
- Behaviour-based and 99% zero-day attack detection
- Fileless and offline attack protection
- Zero Phishing and browser protection
- Ransomware rollback and automated remediation

Investigation, Forensics and Response

- Automated incident and forensic reporting
- MITRE ATT&CK mapping
- Advanced telemetry sensors (process, memory, script, screen, input, DDE)
- PowerShell and script de-obfuscation
- Host isolation and file/process remediation
- C&C blocking and bot remediation
- Posture validation before VPN access

Integration

- Real-time IoC exchange with firewalls
- Lateral movement prevention
- Native integration with APT/Sandbox and other devices
- Shared unified threat intelligence platform

Sandbox (Zero-day malware analysis)

Zero-day capabilities appliances should be installed at Network for the protection against MITRE Att&ck framework or unknown/Advance malware protection, soit is recommended to have such tool at Network level to provide the protection. Thus APT/Sandbox solution should be a part of the solution

Sandbox is a flexible malware/threat-analysis appliance to detect unknown malware. supporting multiple operating systems and file types, to emulate the files in isolated anti-evasive virtual environment. Modern Sandbox technology utilizes AI/machine learning technology to identify and isolate advanced threats in real-time. Sandbox should be equipped with following features

- Detect and protect against Zero-day Malware including ransomware

- Real-time identification of Zero-day Phishing sites including spam and malware-hosted sites
- AI-powered static code analysis identifying possible threats within non-running code
- Deep learning powered VM-Less emulation of Windows executable codes (PEXBox)
- Network threat detection in sniffer mode. Identify botnet activities and network attacks, malicious URL visits
- Extracts URLs embedded in QR Code
- Scan URLs embedded inside document files
- Concurrent Sandbox instances with multiple Operating System types.
- Speed investigation with built-in MITRE ATT&CK mapping of malware.

Deployment and Analysis

- Fully on-premises sandbox (no cloud malware analysis)
- Detection of APTs, zero-day malware and targeted attacks
- Behavioral, heuristic and CPU-level emulation analysis
- Advanced anti-evasion techniques
- Multi-stage malware detection
- Automatic security control updates
- Stateful attack lifecycle analysis
- Cross-matrix OS and application analysis
- Pre-pop
- Emulated licensed OS and applications
- Scheduled and on-demand reporting with multiple timeframes

Integration and Enforcement

- Bi-directional integration with NGFW
- SSL/TLS deep packet/HTTPS inspection
- Automated IoC blocking
- Inline and out-of-band deployment modes

Threat Extraction and Reporting

- Native Content Disarm & Reconstruction (CDR)/ Threat Extraction
- File size support ≥100 MB
- Wide file format support
- C&C geo-location visibility
- PCAP capture and forensic evidence
- PDF and CSV reporting
- SMTP / SNMP notifications

Performance and Intelligence Sharing

- Minimum 8 concurrent sandbox VMs
- 99% zero-day malware prevention effectiveness
- Native telemetry and real time intelligence sharing with EDR, SASE etc.
- Inline, out-of-band, SPAN, TAP, MTA, ICAP deployment
- SMB, CIFS, NFS support

- 8 Gigabit Ethernet interfaces
- Unified threat intelligence database

Secure Access Service Edge (SASE)

SASE (Secure Access Service Edge) is a cloud-native architectural model that converges both networking and security capabilities into a unified service platform, typically delivered as a cloud solution. SASE integrates multiple security and networking technologies to provide optimized, secure, and scalable access regardless of user location or device.

Core Components of SASE

SD-WAN (Software-defined Wide Area Network):Ensures efficient routing and connectivity between users, applications, and data centers.

SWG (Secure Web Gateway) – Protects users from web-based threats and enforcesweb access policies.

CASB (Cloud Access Security Broker) – Secures cloud application usage, providing visibility and control.

FWaaS (Firewall as a Service) – Delivers scalable firewall protection directly from the cloud.

ZTNA (Zero Trust Network Access) – Restricts access based on user identity, role, and context, following zero trust principles.

Key Attributes

- Cloud-Native Delivery: SASE is built for scalability, elasticity, and performance via distributed points of presence (PoPs) close to users and resources.
- Unified Security and Networking: Integrates security inspection, policy enforcement, and network management, reducing reliance on multiple standalone appliances and simplifying management.
- Identity-Centric and Context-Aware: Shifts the security focus from network location to user, device, risk, and context, enabling granular access controls and policies.
- Optimized for Hybrid Work: Delivers secure, consistent access whether users are on-premises, remote, or accessing cloud resources.

Architecture and Deployment

- SaaS-based solution with all infrastructure costs included
- Centralized, cloud-hosted, web-based management console
- Minimum 99.999% service uptime SLA.
- Full API-based configuration and management
- Minimum 70 global PoPs, with at least 5 PoPs in India, Vendor shall demonstrate equivalent local performance via service-level guarantees" if not meeting 70 PoPs

- Mandatory India-only data residency for data plane, management plane and logs

Licensing and Scalability

- Per named-user licensing
- Up to 5 devices per user at no additional cost
- No additional charges for APIs, agents or throughput
- Dedicated static public IP support without extra licensing

Identity, Access and Posture

- Integration with Azure AD, Okta, Local AD and SAML 2.0 IdPs
- MFA and guest user support
- SCIM-based identity synchronization
- Continuous device posture assessment (Windows and macOS)
- Posture-based policy enforcement

Secure Web Gateway and Threat Protection

- Secure Web Gateway with endpoint-based HTTPS inspection
- Browser security for Chrome, Edge, Firefox and Safari
- Advanced sandboxing, threat emulation and CDR included by default
- Zero-day phishing detection
- Corporate credential misuse prevention
- Safe Search enforcement and AI site access control
- Compliance certifications (SOC2 Type 2, GDPR, ISO)

Data Loss Prevention and SaaS Security

- Upload and download protection for cloud services
- Predefined and custom data types for DLP
- AI platform text scanning

Clipboard, copy-paste, print and save restrictions

- SaaS discovery, misconfiguration detection and automated response

6.1.2.1 General Scope of work

- Complete services for the security solutions including supply, implementation, integration, management, maintenance, support should be provided by the bidder.
- The security solutions shall include all components and subcomponents like cables (such as power cables.), Hardware, Software & Database licenses, Accessories and other components (required for Commissioning of the solution as a part of NIT) should be supplied by the bidder at no extra cost.
- Bidder should adherence to the Service Level Agreements (SLA) and regular monitoring and reporting same to HPGCL.
- The bidder shall ensure that during implementation, the performance, security, etc. of the existing network setup must not compromised.
- The bidder shall integrate all supplied security solutions (EDR, SASE etc) with the existing system.
- The solution deployment should be compliant with CERT-In Cyber Security policies and guidelines and country wide regulations and laws from time to time.

- The bidder shall ensure necessary engagement and deputation of skilled professionals for the smooth implementation of the Project at their own cost.
- The bidder shall provide extensive training for EDR, Sandbox, SASE & other equipment provided in the solution directly from OEM/OEM certified trainer.
- The Firm shall provide the complete comprehensive warranty of solution to ensure the continuous operation and minimizing downtime for maintaining the stability of the system during the entire contract period.
- In case hardware replacement is required, it shall be the responsibility of the Bidder to carry out all necessary co-ordination with the OEMs for all Return of Material related activities for timely replacement of faulty appliances and systems within the due time frame as per relevant SLAs.
- HPGCL may conduct audit of its security setup by CERT-In empaneled agency on periodic or need basis. The bidder shall be responsible for complying with all the audit observations discovered in such audits. It shall be the responsibility of the bidder to carry out closure of the audit points by implementing relevant fixes, updates.
- The Firm shall provide certified training for administrators and users for atleast10 man-days.

6.1.2.2 Deployment of Onsite Resident Engineers

The firm shall deploy 04 no. Onsite Cyber Security Specialists - 01 no. at Managerial level and 03 no. at Engineer level and deployment shall be for 6 days in a week. The minimum qualification of 01 no. at Managerial level shall be Post Graduate in Computers/Engineering Degree with 5 years minimum experience of relevant field and 03 no. at Engineer level shall be Graduate in Computers with 3 years minimum experience of relevant field /Engineering Diploma holder with 5 years minimum experience of relevant field deployed for a period of 5 Years. The Manpower deployed at HPGCL sites shall be well trained and meet the cyber security solution requirements. Bidder needs to bear their boarding and lodging expenses on their own.

Responsibilities of Onsite Resident Engineers

- Discover and control rogue devices (e.g., unprotected or unmanaged devices) and IoTdevices.
- Track applications and ratings
- Discover and mitigate the exploit of system and application vulnerabilities with virtual patching and risk-based proactive policies.
- Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database.
- Protect disconnected endpoints with offline protection.
- Leverage application control to easily add allowed or blocked applications to pre-defined lists. This feature is useful for locking down sensitive systems like POS devices.
- USB device control.
- Escalation of open incidents till resolution of the same.
- Case Tracking, Co-ordination & Follow-up of Incident Analysis, Closure of Incidents, Reporting of the same to competent agency.

- Perform root cause analysis for incidents, mitigation steps and coordinate implementation of controls to prevent recurrence.
- System health monitoring & Performance management.
- Comprehensive monitoring of the deployed solutions.
- In case of any fault / degradation in the performance of the supplied solution, the team shall analyze and rectify the fault/issue.
- Analysis of Logs
- Perform initial analysis for known issues and provide the appropriate recommendations for closure.
- Monitor & Reporting of system components health and take necessary action in case of any observed issue.

6.1.3 Location of Project

The supply, installation & commissioning of cyber security systemwill be doneat following locations of the HPGCL:

Sr.No.	Name of Plant/Office & its Location
1	Panipat Thermal Power Station, Panipat, Haryana
2	RGTPP Khedar, Hisar
3	DCRTPP Yamunanagar
4	WYC Hydro Electric Station, Budhkalan, Yamuna Nagar
5	Corporate Office, Panchkula

The bidders shall visit and examine every site of the HPGCL, at their own responsibility and expenses and obtain all information (including that on the risks, contingencies and other circumstances which may affect or influence the bid) that may be necessary for preparing the bid.

SECTION-V: General Terms & Conditions of Contract.

7.1 **Counter Part Arrangements**: - The agency is required to execute the work at HPGCL sites. As a counterpart arrangement, the concerned officers shall be designated for providing the requisite assistance for the proposed work. All other requirements like boarding, lodging, transportation etc. for their officials shall be borne by the agency.

7.2 **Letter of Award**: - Acceptance of a Bid Proposal by HPGCL shall be communicated by the issue of a letter of Intent (the "Letter of Award").

7.3 **Acceptance Of Letter Of Award and Agreement**: - The successful bidder shall accept the Letter of Award within 7 (seven) days from the date of issue of the Letter of Intent by returning a duly signed copy thereof and shall enter into the Contract Agreement with HPGCL within 15 days from the date of issue of work order, on a non-judicial stamp paper of requisite value with HPGCL. The stamp duty is to be borne by the bidder. The bidder shall also furnish PBG along with the contract agreement and shall be kept in full force and effect for the full term of the Contract Agreement. The period of contract agreement shall be effective for the full term of Contract Agreement.

7.4 **Subletting of Assignment:** - The agency shall not assign or transfer the Contract Agreement, in whole or in part, to any sub-contractor or any other party i.e. no sub-letting of the contract is allowed.

7.5 **Force Majeure**: If the agency is prevented from performing any of its obligations under the Contract Agreement due to causes such as fire, Acts of God, or elements, embargoes, governmental orders, the agency shall be excused from the non-performance of its obligations during the period that such cause continues to exist.The agency shall however, inform the corporation by registered post about such acts at the beginning and end of the above causes of delay within ten days of occurrence &cessation of such force majeure conditions.

7.6 **Indemnity** If, for any reason or resulting from any cause whatsoever, any statement, representation or warranty set forth in the Bid Proposal and Contract Agreement is found to have been materially incorrect or untrue when made, in breach or fails to prove to be true, the agency shall be fully liable to any and all liability, damage, any third party claims, costs and expenses including legal fees arising from such misrepresentation, breach or incorrect statement. The agency

shall indemnify and the keep indemnified the Employer fully and hold harmless against any and all liabilities, costs, expenses including legal fees, third party claims of infringement of copyright, trademarks, trade names, patents and other intellectual property rights subsisting in or used in connection with the Consultancy Assistance to Haryana Power Generation Corporation Limited (HPGCL) including all documentation and manuals relating thereto including any original authorship of further developmental works or derivative works made. The agency shall indemnify the Employer against all actions, suits, claims, demands, costs or expenses arising in connection with death or injuries suffered by persons employed by the agency under any applicable Law for the time being in force.

7.7 **Compliance with Laws**: - The agency shall conform to and comply with all applicable Laws of the state or central government and / or any Legal Authority, bye-laws of the Employer and all other local authorities including without limitation to industrial and labour laws and tax laws.

7.8 **Penalties for Delay**: -

PART-A

In case of failure to complete supply of equipment i.e. PART-Ain time the penalty shall be levied @0.5 % per week or part thereof of the total contract price subject to maximum of 10% of total contract price subject to force majeure.

PART-B

The contractor shall ensure timely completion of the job as per stipulated completion period. In case of delay in completing the work/job, the penalty for delay will be imposed @ 1% of the service part value of the contract per day or part thereof subject to maximum of 10% of the service part value of the contract.

7.9 **Service Level Agreement**

The comprehensive warranty is required for 5 years which includes onsite warrantee as well as comprehensive maintenance of the complete system. The scope also comprises the deployment of Engineer to undertake the routine/breakdown maintenance. In case of odd hour's failures and emergencies even on holidays and Sunday, normal service is to be rendered by the Bidder. In case the bidder fails to rectify the fault in allowable time, the penalty would be imposed as per following manner: -

Service Level Agreement Bidders need to strictly adhere to Service Level Agreements (SLA). Services delivered by Bidder should comply with the SLA

mentioned in the table below. SLA will be calculated quarterly. SLA violation will attract penalties. Availability means the time for which the services and facilities are available.

Availability is defined as (%) = (Total hours in one quarter – Downtime) * 100

Total hours in one quarter

SN	Service Area	Acceptable Service Level	Penalty(as per Part(ii))
SASE			
1	SASE Solution Uptime. Uptime % calculated on a quarterly basis for SASE.	System Availability 99.9 % and above	No deduction
		98% to 99.9	1 % of quarterly payment
		95% to 97.99%	2 % of quarterly payment
		90% to 94.99%	3 % of quarterly payment
		Less than 90%	5 % of quarterly payment
2	Incident response and resolution	For any SASE related incident that is reported acknowledgement should be provided within 30 mins and the incident to be closed within 8 hours 99.9 % and above	No deduction
		98% to 99.9	1 % of quarterly payment
		95% to 97.99%	2 % ofquarterly payment
		90% to 94.99%	3 % of quarterly payment
		Less than 90%	5 % of quarterly payment
3	Provision of SASE and updates	SASE updates to be provided and installed within one week of its release 99.9 % and above	No deduction
		98% to 99.9	1 % of quarterly payment
		95% to 97.99%	2 % ofquarterly payment
		90% to 94.99%	3 % of quarterly payment
		Less than 90%	5 % of quarterly payment
Other components			
	Any issue reported towards Hardware/Software means issue related to hardware failure or non functioning: Malfunctioning, firmware crash reported	Resolution of the issue by rectification or replacement within 8 hours	No deduction
		After 8hours	1 % of quarterly payment
		After 2day	2 % of quarterly payment
		After 5 days	5 %of quarterly payment
		After 7 days	10 %of quarterly payment

Note:

1. It may be noted that over and above the penalty, during the down time all the responsibilities will lie on the Bidder for any security issues happened due to system down.
2. Contract value means basic value of the contract exclusive of taxes and duties, if charged separately
3. In case of non-availability of Engineer, If bidder fails to provide the suitable substitute of the Engineer, Rs.2000/- per day Plus an amount equal to the one day emoluments be deducted over and above the penalty during non-availability of Engineer.

7.10 **Arbitration**: -

7.9.1 All matters, questions, disputes, differences and/or claims arising out of and/or concerning, and/or in connection with, and/or in consequence of, and/or relating to any contract under these Regulations, whether or not obligations of either or both the Supplier and the Corporation under that contract be subsisting at the time of such dispute and whether or not the contract has been terminated or purported to be terminated or completed, shall be referred to the sole arbitration of Appointing Authority. The award of the Arbitrator shall be final and binding on both the parties to the contract.

7.9.2 The objection that the Arbitrator has to deal with matters, to which the contract relates, in the course of his duties or, he has expressed his views on any or all of the matters in dispute or difference, shall not be considered as a valid objection.

7.9.3 The Arbitrator may, from time to time, with the consent of the parties to the contract enlarge the time for making the award. The venue of the arbitration shall be the place from which the acceptance of offer is issued or such other place as the Arbitrator, in his discretion, may determine.

7.9.4 All arbitration proceedings under this Regulation shall be governed by the provisions of the Arbitration and Conciliation Act, 1996 and the Rule there under, with any statutory modifications thereof for the time being in force.

7.11 **Price, Taxes, Duties and Evaluation:-**

7.10.1 Price offered in financial bid will be fixed throughout the contract period and no escalation will be allowed.

7.10.2 Any variation, up or down, in taxes and duties or any new levy introduced

subsequent to bid opening will be considered applicable.

7.10.3 The Tax liability, if any, on deputation of the agency personnel shall be borne by the agency and shall be responsibility of the agency as per Tax laws of India.

7.10.4 The contractor shall pay taxes, duties, fees, GST and other impositions as may be levied under the applicable laws in India, the amount of which is deemed to have been included in the quoted price.

7.10.5 Amount payable to the contractor shall be subjected to deduction of TDS (Tax deduction at source) or any other applicable taxes as per tax laws of India. The Contractor shall be responsible for assessment of his income as per the applicable Income tax laws in India. The Owner will not accept any liability on account of Tax/addition tax/penalty/Interest burden etc. for assessment of his taxable income by Indian Income Tax Authorities.

7.10.6 The personal income tax of overseas agency, if payable shall be paid by the overseas agency directly. Owner shall neither be liable to pay the income tax nor for filling the tax return for overseas agency.

7.12 **Jurisdiction of Courts**: - The courts at Panchkula shall alone have exclusive jurisdiction to decide any dispute arising out of or in respect of the contract.

7.13 **Termination of Agreement**: - If the work entrusted is not proper and to the satisfaction of HPGCL and if the work of the agency continues to be unsatisfactory, the agreement shall be terminated by HPGCL by giving 15days' notice at any time during subsistence of this agreement. The same will be entrusted to another agency and the extra expenditure incurred by HPGCL, the same will have to be borne by the existing agency.

7.14 **Inspection:-**The Supplier shall at its own expense and at no cost to the Purchaser carry out all inspection to ensure that the Goods and Related Services are complying with the functional parameters, codes and standards specified in the Scope of Work, to the satisfaction of the Purchaser before dispatch. Whenever the Supplier is ready to carry out any such inspection, it shall give a reasonable advance notice, including the place and time, to the Purchaser.

7.15 **Negligence & Risk Coverage**: - If the agency contravenes the provisions of this contract or fails to provide efficient services or refuses to comply with any reasonable order given in writing by the Controlling officer of the Employer or his authorized representatives, a one week notice shall be served upon him to correct

himself and to execute this contract in true spirit. If an agency fails to take notice of such notice served upon him, the Employer shall be at liberty to take the work wholly or in part, out of the agency hands and re-contract with any other person(s) at the cost of the agency. Any extra expenditure incurred by the Employer on such re-contracting shall also be recoverable from the agency, in addition to the HPGCL right or claim for liquidated damages. It shall also be lawful for the HPGCL to forfeit either in whole or in part, in its absolute discretion, the security deposit furnished by the agency. Forfeiture of the security deposit shall be without prejudice to the right of the HPGCL to recover any further amount of any liquidated and / or other damages to the maximum of 10% of the total contract value, undue payment or overpayment made to the agency under this contract or any other contract.

7.16 **Set Off: -**Any sum of money due and payable to the supplier under a contract (including security deposit returnable to the supplier) may be appropriated by the Corporation and set off against any claim of the Corporation for the payment of a sum of money arising out of that or any other contract entered into by the supplier with the Corporation**.**

7.17 **Risk-Purchase:-**In addition to the provisions defined in this bid document, the Purchaser will have the right to take action as per following:

7.15.1 In case of delay or non-supply of any or all the material or related services on the dates they are due, the Corporation will have a right to refuse to accept such delayed supplies or services and to make the purchase of the material or services so delayed or not supplied from any alternative source or through departmental manufacture, at the sole risk and cost of the supplier. Any extra expenditure incurred on such purchase or departmental manufacture shall be recoverable in full from the supplier in addition to the Corporation's right or claim for applicable liquidated damages or penalty.

7.15.2 The purchasing authority may cancel the purchase order due to non – fulfillment of its terms (i.e. delivery, non-working, etc.) by the supplier and give notice for recovering the damages applicable to such non-fulfillment.

7.15.3 Where risk purchase action is proposed to be taken, a legal notice should be served by the purchasing authority on the supplier by registered post

bringing his defaults to his notice pointedly and asking him to complete all pending supplies immediately, and in any case, within the specified period, (a reasonable period to be specified by the purchasing authority in the notice), failing which the Corporation shall reserve the right to effect the risk purchase at his sole risk and cost, besides levying and recovering liquidated and /or other damages admissible under the contract, or to cancel the contract at its sole discretion and recover the damages for non-fulfillment or unsatisfactory execution of the contract. He should be asked to acknowledge the receipt of the notice immediately. In case he again defaults, he should be issued a further legal notice stating that as he had failed to fulfill his part of the contract by delaying deliveries, the purchasing authority was issuing a tender for the purchase of the quantities or services not delivered by him and any extra cost including the cost of re-tendering will be recoverable from him in addition to the liquidated damages leviable in terms of the contract. He should be asked to acknowledge the receipt of this notice also. Immediately, thereafter, a notice inviting tenders should be issued and a copy of the NIT should also be sent to the supplier giving him an opportunity again to participate in the tender. On receipt of tenders and their comparison, a copy of the purchase order issued should also be sent to him,In case he himself is the person on whom the order is to be placed, he will be entitled only to receive the payment as per the original purchase order. On completion of the supplies or services by the firm from whom this purchase is effected, a full account, including loss incurred on risk purchase, liquated and / or other damages claimable under the contract, should be sent to the supplier against whom the risk purchase is effected demanding legally that he shall make good the amount within a reasonable period (to be specified). Failing payment of the same by the supplier, the amount of the claim shall be recovered from his outstanding dues and / or security deposits against the relevant contract or any other contract in operation, and for the balance, due process of law shall be initiated.

7.15.4 For deciding upon the question of acceptance of delayed supplies or services, and /or of grant of extension in the delivery dates against the supplier's application in this behalf, or enforcing risk purchase action or even cancelling the purchase order in such terms, the powers of purchasing

authority shall be exercised by the Committee constituted by HPGCL in cases where the Whole time Directors, HPPC, BOD or other higher authority are the competent purchasing authority.

7.18 **Damage to Equipment or to any Person or any Third Party: -** The agency shall be liable for any loss / damage caused to the property, equipment or to any employee of HPGCL or to third party due to their negligence or willful misconduct. HPGCL shall recover the cost of such damage from the agency. If claims are lodged against HPGCL by third parties for compensation of damage or loss caused by agency fault, the consultancy firm / bidder shall keep indemnified HPGCL against all claims raised by third parties.

7.19 **Confidentiality**: - The terms of the bid, Letter of Intents, Contract Agreement and all information disclosed by the HPGCL and obtained by the agency in connection with the Consultancy Assistance to HPGCL shall remain the exclusive property of the HPGCL and shall not be disclosed by the agency to any third party other than without the prior written consent of the HPGCL.

7.20 The language of the Contract Documents shall be English.

7.21 The laws that apply to the Contract are the laws of Union of India.

7.22 The currency of the Contract is Indian Rupees.

7.23 **INSURANCE OF WORKERS: -**

The contractor will be solely responsible for any liability for his workers in respect of any accident, injury arising out and in course of contractor‘s employment.

7.24 **SAFETY RULES: -**

The Firm shall have to comply with all the provisions of safety rules. A penalty of Rs.200/- per day per head shall be imposed if the workers of contractor are found to be working carelessly without proper protective equipments in unsafe conditions. Against violation of any other clause, a penalty of Rs 500 /- per violation (minimum) shall be levied. In case of repeated violation of serious nature resulting in various serious accident or direct loss to the corporation /threatens to cause severe consequences, higher penalty rates may be imposed including suspension/ termination of the contract. If any action is initiated by Chief inspector of factories, Chandigarh or any other authority against occupier/factory manager or any other authority of HPGCL in case of any

fatal/non-fatal accident or any other violation of factory act, 1948, Pb. Hr. factory rules, 1952 or any other industrial or labour act, the contractor shall be liable for the same and also to deposit the amount of fine/penalty if any. In case of default action as deem fit shall be initiated against the contractor. A safety clearance certificate on quarterly basis from the chief safety officer shall be obtained by the contractor and has to be attached along with the bill. This office reserves the right to claim adequate compensation from the contractor on account of any damage caused to the plant & equipment handed over to him for execution of the work, due to careless handling or negligence on the part of the contractor.

7.25 **Factory Act/Minimum Wages Act/Insurance Act/ EPF Act Etc.**

Strict adherence of various applicable labour laws like the Factories Act, Minimum Wages Act, ESI Act, Payment of Wages Act, the Workman's Compensation Act, EPF Act, Contractor labour (Regulation & Abolition) Act, 1970 and all other statutory requirements as amended from time to time to the entire satisfaction of Central/State Govt. Authorities, shall be the responsibility of the Contractor and he shall have to make good loss, if any, suffered by HPGCL on account of default in this regard by the contractor.

7.26 **Idle Labour Charges**

No idle labour charges will be admissible in the event of any stoppage caused in the work resulting in contractor's labour being rendered idle due to any cause.

7.27 **Over Run Charges**

No overrun charges shall be paid in the event of the completion period being extended for any reasons.

7.28 **Watch & Ward**

The watch and ward of T&P and other material will be the responsibility of the contractor.

7.29 **Eligibility Of The Black Listed Firms To Participate In NIT**

The firms who have been blacklisted by HPGCL or any other Centre or State Power Utility/ Board or Corporation/ or any other Thermal/Hydro Elect. project shall not be eligible to bid against the NIT of HPGCL, However;

(i) In case the blacklisting of the firm is for a specific plant and not for the organization as a whole then such blacklisting will not tantamount to ineligibility of the bidder.

(ii) Blacklisting of the firm by any unit of the HPGCL shall be considered as ineligibility of the firm at any other project of HPGCL.

(iii) In case any firm was blacklisted for a limited period in past by any organization and presently such blacklisting has removed by such organization then it will not tantamount to ineligibility of the bidder.

(iv) Firm has to certify itself for its eligibility with supporting documents to participate in the NIT stating that it has not been blacklisted by any organization presently, however in case at a later stage such certification found wrong then it will lead to misrepresentation of the facts and the firm shall be treated as blacklisted on this ground and action shall be taken as per HPGCL regulation.

7.30 **GST DOCUMENTS & UNDERTAKING:**

All Prospective bidders to submit copy of Registration Certificate under GST Act.

The following undertakings (on the letter head of the bidder) to be made part of mandatory documents to be submitted by all bidders:-

a) GST registration is valid as on date.

b) No default has ever been made by bidder in filing the various GST returns and deposit of GST dues with the department.

c) Bidders having multiple registrations under GST will submit undertaking for each & every GST number. A default under a GST number even if the GST number pertains to some other state, will make the bidder ineligible to participate in tender.

The successful bidder will also submit the following undertakings in addition to above immediately after issue of work order and with submission of each & every bill unless mentioned otherwise:-

d) Undertakings mentioned at (a), (b) and (c).

e) A CA certificate regarding validity of GST registration will be submitted every six months during the tenure of the contract.

f) Bidder will submit copies of GSTRI and GSTR 3B/challans as evidence to deposit of GST with certification that GST collected from HPGCL, to be specified in exact rupees, has been paid to Govt. vide this challan (specifying the challan no. & date of deposit) and returns filed (date of filing of return) includes the transaction of supply of Good or / and services to HPGCL.

g) Bidder will inform immediately the HPGCL about initiation of any proceeding (if any) against him under the GST laws which may result in suspension or cancellation of GST number of bidder.

h) Undertaking to indemnify the HPGCL in case of any financial implication on HPGCL due to non compliance of prescribed obligation under the GST Law on part of the supplier / bidder.

7.31 Any other Terms and conditions not specifically mentioned here but required for said work shall be guided by HPGCL Purchase regulations 2015 available on HPGCL websitewww.hpgcl.org.in.

7. SECTION-VI: Payment Terms.

8.1 PRICE BASIS

Delivery at Place (DAP) basis i.e. (Delivered at respective HPGCL sites) inclusive of all taxes and duties, freight & insurance upto respective locations. Evaluation will be done on all inclusive prices.

8.2 PAYMENT TERMS

Supply of Material (PART A):

- 90% payment of supply part shall be made after 21 days of receipt of 100% material at Stores site in good condition and on submission of all the requisite documents as per work order.
- Balance 10% after 21 days after successful installation & commissioning.
- The Security Deposit shall be 2% of the Part-A of the Contract value for faithful execution of the contract. The EMD already deposited by successful bidder shall be converted into the security deposit of Part–A and balance amount if any shall be deducted from the first invoice.
- No payment will be made for goods rejected on testing done at Supplier end or by Purchaser.

Services Part (PART B):

Part B(i): Installation and Commissioning Charges

- 90% payment shall be made within 21 days of successful installation & commissioning.
- 10% of balance amount of installation and commissioning shall be kept as security deposit which shall be released 30 days after completion of the contract period of 5 years post installation & commissioning.

Part B(ii): Onsite Resident Engineer

- The payment will be made on quarterly basis after satisfactory completion of the jobs for 5 years.

You shall submit the RTGS details (i.e. IFSC code, Bank A/c No., Name & Branch of Bank) and GST/PAN/TIN details along with the bills submitted to HPGCL.

8.3 DELIVERY SCHEDULE

Supply, Installation & Commissioning of EDR, Anti-APT/Sandbox, Secure Access Service Edge (SASE) including all Equipment/deliverables at HPGCL sites to be made within 150 days from the date of issue of Work Order. Bidder has to submit

Pre- Delivery Note to HPGCL before material delivery and the material shall be routed through stores of respective Power plants.

8.4 **PERFORMANCE BANK GUARANTEE (PBG)**

Successful bidder shall submit 10% of the Total Contract value as Performance Bank Guarantee in the form of BG (Bank Guarantee) within 15 days of issuance of Order. The duration of Period shall cover the entire contract period plus additional 3 months. PBG can be executed with any Nationalised Bank or Scheduled Bank however Nationalised Bank is preferred.

8.5 **QUANTITY VARIATION**

The quantum of any items of supply part mentioned in schedule of requirements of scope of work may increase/decrease to any extent, as per the requirement, subject to the limit that the total contract value shall not exceed by 10% of the total contract value.

In case, any quantity exceeds or is less than the quantity in bid price schedule, the payment for the executed quantity shall be paid on pro-rata basis, for the actual quantities consumed / for which the installation is carried out through the Bidder on Certification by Technical Representative of HPGCL and the unused quantity will be returned back and the Payment disbursed against unused quantity will be reconciled in the next payment.

8. SECTION-VII: SCHEDULE OF REQUIREMENT AND PRICE BID SCHEDULE

Sr. No	Description of Items	UoM	QTY	Amount excl. Taxes (in INR)	Taxes (in INR)	Total Amount incl. Taxes (in INR)
PART A: Supply Part						
1	End Point Detection & Response (EDR) for 850 Devices On-Prem Solution including Hardware along with Licenses, OEM Comprehensive warranty & OEM 24x7 premium support for 5 years.	Unit	1			
2	APT/Sandbox for 4 locations i.e HPGCL Corporate Ofiice, Panchkula; PTPS, Panipat; RGTPP, Khedar, Hisar & DCRTPP, Yamunanagar including Hardware along with Licenses, OEM Comprehensive warranty & OEM 24x7 premium support for 5 years.	Unit	4			
3	Secure Access Service Edge (SASE) for 850 Devices including Hardware along with Licenses, OEM Comprehensive warranty & OEM 24x7 premium support for 5 years.	Unit	1			
4	Any other item required for implementation of solution	Lot	1			
	Total PART A					
PART B(i) : Installation and Commissioning						
5	System Implementation of Complete Solution at HPGCL sites.	Lot	1			
	Total PART B(i)					
PART B(ii) : Onsite Resident Engineer						
	The firm shall deploy 04 no. Onsite Cyber Security Specialists - 01 no. at Managerial level and 03 no. at Engineer level and deployment shall be for 6 days in a week. The minimum qualification of 01 no. at Managerial level shall be Post Graduate in Computers/Engineering Degree and 03 no. at Engineer level shall be Graduate in Computers/Engineering Diploma holder for 5 Years.					
6	Onsite deployment for 1st year.	Lot	1			
7	Onsite deployment for 2nd Year.	Lot	1			
8	Onsite deployment of for 3rd Year.	Lot	1			
9	Onsite deployment for 4th Year.	Lot	1			
10	Onsite deployment of for 5th Year.	Lot	1			
	Total PART B					
	TOTAL CONTRACT VALUE i.e PART (A) + PART (B)					

*The payment for PART B shall be paid on the quarterly basis.

9. TECHNICAL SPECIFICATIONS.

1. Endpoint Detection and Response (EDR)

Agent & Licensing

- Unified Agent Architecture: The proposed solution shall use a purpose-built, unified agent for comprehensive endpoint protection, offering threat prevention, attack investigation, access control, sandboxing, and web protection capabilities. Multiple agents are not acceptable.
- The proposed solution shall offer all the features, specified herein, in a single unified installation. Installation of multiple agents to achieve the requirement is not acceptable.
- Licensing Model: The solution shall be licensed for at least 850 client machines and shall leverage both signature-based and signatureless security controls using advanced AI/ML-based models.

Protection Mechanisms

- Core Protection Features: The solution should include the following integrated protection mechanisms:
  i. Anti-Ransomware protection
  ii. Behaviour-based protections
  iii. Anti-exploit
  iv. Anti-Bot
  v. Anti-malware
  vi. Forensics Collection & automated reports
  vii. Web Protection
  viii. Sandboxing
- Zero-Day Ransomware & Remediation: The solution will protect against existing and zero-day ransomware without requiring signature updates. It shall also remediate and restore files encrypted during a ransomware attack.
- ML Model Updates: Any Machine Learning (ML) models used by the endpoint should be frequently updated to ensure protection against novel zero-day attacks.
- Static Detection & Hashing: The solution's Static Detection Engine shall monitor file access and check file reputations based on ssdeep/Fuzzy hashing.
- Behavioral Analysis: The solution will leverage multiple sensors to effectively and uniquely identify generic malware behaviors as well as malware family-specific Fuzzy hashing.
- Online/Offline Protection: The solution will immediately prevent or detect malicious behaviors regardless of whether the machine is online or offline.
- Advanced Attack Detection: The solution will detect and prevent fileless attacks based on scripting and shall detect zero-day local privilege escalation (LPE).
- Exploit Prevention: The solution will detect and prevent exploitation techniques used against trusted software.
- Vulnerability Protection: The solution has the capability of blocking new RDP RCE attacks like BlueKeep on unpatched systems.
- Zero-Day File Identification: The solution shall be able to identify zero-day files even if they are unfamiliar to any reputation service.
- C&C Communication Blocking: The solution will identify and block outbound communication to malicious Command and Control (C&C) sites.
- Full Remediation: Upon an identified bot attack, the solution will completely remediate the attack, leaving the endpoint clean and unharmed.

- Malware Scope & Central Management: The solution will protect the computer from all kinds of malware threats (worms, Trojans, adware, keystroke loggers) and manage detection and treatment centrally.
- Proxy Updates: The solution should be able to use a dedicated client as a proxy for anti-malware signature updates for offline clients or to limit bandwidth usage.
- Should support zero-Phishing, Browser Protection, Remote Access VPN within the same agent.

Investigation & Forensics

- Automated Incident Analysis: The solution will automatically create an incident analysis for every detection/prevention, including process execution trees that persist across reboots if relevant.
- Forensic Reporting: Forensic reports will automatically identify the malicious activity entry point and highlight potential damage, remediation actions, and the entire chain of attack.
- Third-Party Integration: The solution will enhance third-party anti-malware or security detections by automatically building and visualizing incident reports.
- Script Un-obfuscation: Forensic reports will log, present, and un-obfuscate PowerShell scripts used during an attack.
- Sensor Requirements: The solution shall include the following sensors: Remote Execution, Service Creation, Process Discovery, Application Window Discovery, Scheduled Task, Screen Capture, Input Capture, and DDE (Dynamic Data Exchange).
- MITRE ATT&CK Mapping: The solution will create an incident report that displays the incident mapped against the MITRE ATT&CK Matrix.
- Host isolation and file/process remediation
- C&C blocking and bot remediation
- Posture validation before VPN access

Response & Web Security

- File/Process Remediation: The solution will allow for the remediation of any file or process found through the EDR platform.
- Forensic Analysis Access: The solution will allow for forensic analysis and reporting of any indicator found through the EDR platform.
- Phishing Protection: Solution shall detect and block access to phishing sites by scanning all form fields, not relying solely on URL reputation-based techniques.
- Account Takeover Prevention: The solution should provide protection for account takeover attacks and alert users on the reuse of corporate passwords.
- Browser & Search Security: The solution will scan for malicious JavaScript embedded within sites and enforce "Safe Searching" features when using Google, Bing, and Yahoo search engines.
- Signatureless Browser Protection: The solution should have intelligence to detect and prevent browser-based attacks without dependency on signatures.

Integration & Posture Enforcement

- Real-Time IoC Exchange: Both the Endpoint solution and the existing Firewall should exchange IoCs (hashes, domains, IPs, URLs) in real-time for unified threat blocking.
- Posture Validation: Endpoint security posture (AV status, encryption, patches) should be validated with the existing firewall before VPN login is permitted.
- Lateral Movement Prevention: Endpoint detections shall feed into the firewall to block an infected host’s east-west traffic across internal networks.

- Compliance Enforcement: The solution will enforce endpoint computers to comply with organization-defined security rules, marking non-compliant machines and applying restrictive policies to them.
- Native integration with APT/Sandbox and other devices.
- Shared unified threat intelligence platform
- Solution must use one threat intelligence database across SASE, EDR, Sandbox etc. with unified indicator sharing or native integration with similar threat intelligence technology.

2. APT/ Sandbox :

Integration & Traffic Inspection

- Bi-directional Integration: The solution shall communicate bi-directionally with existing Next-Generation Firewalls (NGFW) for automatic blocking and threat updates.
- SSL Inspection: The solution shall support deep packet inspection of SSL-encrypted traffic (including HTTPS) for both inbound and outbound connections.
- APT Detection: The solution shall provide detection, analysis, and remediation capabilities against APT and SSL-based APT attacks.

Detection & Analysis Capabilities

- On-Premise Analysis: The solution shall employ an on-premise (not cloud-based) analysis engine using virtual execution to detect zero-day and unknown threats, without relying solely on signatures.
- Comprehensive Threat Detection: The solution should detect and prevent advanced malware, zero-day attacks, spear-phishing attacks, drive-by downloads, watering hole attacks, and targeted APTs without relying on just a signature database.
- Real-Time Dynamic Analysis: The solution shall perform dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks. No files should be sent to third-party systems or cloud infrastructure for analysis.
- Anti-Evasion: Built-in anti-evasion engines shall be capable of detecting packed, obfuscated, or time-delayed malware.
- Automated IoC Blocking: Real-time integration with existing blades like IPS and Anti-Bot for automatic IoC blocking without manual effort.
- CPU-Level Emulation: The sandbox shall support CPU-level emulation capable of detecting packed, obfuscated, delayed-execution, and anti-VM evasive malware.
- Multi-Stage Threat Confirmation: The solution shall automatically detect and confirm multi-stage zero-day malware and targeted attacks without prior knowledge of the malware.
- Automated Security Control Updates: The solution shall automatically update security controls with newly detected malicious indicators without requiring admin intervention or manual policy pushes.
- Stateful Attack Analysis: The solution should utilize stateful attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.
- Cross-Matrix Analysis: The solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of predefined applications.
- Scheduled and on-demand reporting with multiple timeframes

Platform & File Handling

- Licensed OS & Applications: The solution shall include pre-populated, licensed copies of operating systems and applications/software (e.g., Microsoft Office). There should be no requirement for the customer to purchase additional licenses.
- File Size Support: The system should be able to support file sizes up to 100 MB or higher.
- Native Threat Extraction (CDR): The solution shall support Threat Extraction (Content Disarm & Reconstruction), enabling the immediate delivery of a sanitized, safe version of potentially malicious files by removing active content and embedded objects. CDR shall be natively integrated with the sandbox solution and provide instant file sanitization without requiring separate licenses, appliances, or modules.
- File Format Analysis: The proposed solution should have the ability to analyze, detect, and block malware in common file formats, including (but not limited to) pptm, xlsm, vbe, ppsx, docm, cmd, ole, xlsx, pptx, uue, hwp, scr, xz, ppt, doc, xltm, xar, jar, wsh, pkg, pps, pdf, slk, rar, dmg, tgz, potx, zip, exe, tar, PIF, rtf, lzh, tb2, macho, swf, and .vba files.
- Packet Capture Storage: The solution should capture and store packet captures (PCAPs) of traffic relevant to the analysis of detected threats.

Reporting & Monitoring

- Geo-Location Reporting: The solution should display the geo-location of remote Command and Control (C&C) servers via native integration with the existing firewall.
- Detailed Incident Reporting: The solution should report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols, and infection severity of the attack.
- Notification Protocols: The solution should send both summary and detailed per-event notifications utilizing SMTP or SNMP protocols.
- Inbound/Outbound Blocking: The solution shall block inbound malicious exploits delivered via a web channel and outbound callback communications when deployed in inline or out-of-band mode.
- Protocol Support: The solution should support SMB, CIFS, and NFS protocols for file sharing and transferring.
- Scan Visibility: The solution should provide visibility into scan histories for each file, including statuses such as aborted, completed, or in progress.

Deployment & Scalability

- Deployment Modes: The APT solution shall support deployment as an inline MTA, ICAP, and via SPAN/TAP mode.
- Reporting Formats: The solution should provide reports in PDF and CSV formats (minimum).
- Anti-VM Evasion: The solution shall have anti-evasion capabilities to prevent malware from detecting that it is running/executed in a virtualized environment.
- SIEM Integration: The solution should support SIEM log integration.
- Flexible Reporting: The solution should be able to schedule reports and provide the flexibility to generate on-demand reports (daily, weekly, monthly, yearly, or specific time ranges).
- Minimum Interfaces: Minimum number of interfaces: 8x GE RJ45 Ports.
- VM Capacity: A minimum of 8 analysis VMs shall be available from day one.

- OS Support: It shall support sandbox analysis for multiple Windows operating systems.

Threat Intelligence & Enforcement

- Native Firewall Integration: The sandbox solution shall support native integration with existing firewalls.
- Automated Inline Enforcement: Sandbox verdicts shall automatically enforce protection inline across Endpoint and Network security controls without relying on external SIEM/SOAR systems..
- Seamless Telemetry Sharing: Sandbox, EDR, and SASE shall natively share telemetry in real-time without connectors, API integration, or third-party middleware.
- Unified Policy Enforcement: Sandbox verdicts shall be automatically enforced across SASE and Endpoint controls without policy duplication or manual synchronization.
- Unified Threat Intelligence Database: The solution shall use one shared threat intelligence database across SASE, EDR, Sandbox etc. with unified indicator sharing or native integration with similar threat intelligence technology.

3. Secure Acess Service Edge (SASE)

General & Deployment

- Deployment & Billing Model: The solution shall be SaaS-based. All cloud infrastructure costs, including gateway compute scaling, shall be included in the SASE subscription without separate consumption billing.
- Management Console: Management shall be cloud-hosted, web-based, and consolidated for all SASE services.
- Service Level Agreement (SLA): The proposed solution shall have 99.999% service uptime SLA for the SASE/SSE solution, documented in writing or a public agreement.
- API Management: The solution should support APIs to configure and manage networks, gateways, regions, users, groups, tunnels, and other functionalities.
- Global & Regional Presence: The solution should have a minimum of 70+ Points of Presence (PoPs) globally, with at least 5 or more located in India.
- Static IP Support: The solution shall support a dedicated static public IP address for the tenant/gateway at no additional cost or license fee.
- Client Platform Support: The solution should support operating systems like Windows, macOS, Linux, Ubuntu, RedHat, Android, Chromebook, and iOS for private access, and Windows, Linux, and macOS for internet access.
- Mandatory India-only data residency for data plane, management plane and logs

Licensing & User Management

- User-Based Licensing: Licensing shall be based on the number of unique users, assuming a single user may utilize multiple devices.
- Device Per User Limits: Each user should be able to use up to 5 devices under the same license. The license model shall be strictly per named user with no additional charges per device, agent, or throughput.
- No additional charges for APIs, agents or throughput
- Agent Version Control: The administrator shall be able to control agent version updates.

- Automated Client Updates: Client software should auto-update directly on user devices based on defined policies.
- Identity Provider (IdP) Integration: The platform shall support Azure AD, Okta, Local AD, and any SAML 2.0 identity provider for authentication as an IdP.
- Guest & MFA Support: The solution should support platform access for guest users (via email and password) and multi-factor authentication (MFA).
- Hybrid User Database Support: Shall support simultaneous use of internal/local database users (for third parties/contractors) and IdP-integrated users.
- Identity Synchronization & Integration: The solution should support identity group integration/synchronization. Integration with IdP, MFA, and identity posture assessment shall be included without requiring separate IAM or MFA licensing.
- SCIM Integration: The solution shall have SCIM integration capabilities with Azure AD and Okta.

Network & Security Functionality

- Split Tunnelling: The platform shall support split tunnelling, including both "include" and "exclude" options, and support for both IP addresses and FQDNs.
- On-Device Network Protection: The solution shall support direct internet access through on-device network protection without routing all traffic back to a PoP.
- Browser Security: Should support browser security for protection against zero-day phishing, corporate credential reuse, malicious file downloads, and data leakage (including through GenAI apps) without compromising speed or privacy.
- Tenant Restrictions: Shall provide tenant restrictions for O365 and Google Workspace environments.
- SaaS Security Posture Management (SSPM): Should support SaaS Security for complete mapping of the SaaS ecosystem, including misconfiguration detection, timely alerts, and automated threat response.
- Data Sovereignty: All data plane (log storage), management plane (policy controller), and PoPs shall be located within the Indian Geo-boundary, without exception.
- URL Categorization: The solution shall have inbuilt categories to select/provide access to specific users/groups and the ability to create custom URLs as required by the business.
- Bypass Rules: There shall be an option to create bypass rules to exclude scanning for trusted domains like Microsoft and Google Drive.
- Localized Web Content: The internet access solution shall support accurate localized web content even in cities without local PoP infrastructure.

Secure Web Gateway (SWG) & Threat Protection

- Offline SWG Functionality: The local agent shall support SWG functionality even when the client disconnects from the VPN.
- HTTPS Inspection & Privacy: SWG functionality shall support HTTPS inspection, performed directly on the agent to maintain user privacy.
- Automated Secure WiFi Access: Client-based access shall automatically secure traffic over unprotected WiFi networks (when detected, the client shall route all traffic via VPN, overriding defined split tunneling rules).
- Supported Browsers: The solution shall support Chrome, Edge, Firefox, and Safari browsers.

- Content Disarm & Reconstruction (CDR): The solution shall have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros, and active content.
- Original File Access: When scrubbing via CDR, the original file shall remain accessible to the end user if deemed benign by the sandbox.
- File Emulation: Incoming files shall be emulated via sandboxing for potentially malicious content.
- Integrated Threat Features: Advanced sandboxing, threat emulation, CDR, and threat intelligence shall be part of the standard SASE license, not an optional upgrade.
- Zero-Day Phishing Detection: The solution will detect zero-day phishing sites that request user credentials, even if unknown to reputation engines.
- Malicious URL Blocking: The solution shall block users from browsing to known malicious URLs or domains.
- Corporate Credential Protection: The solution shall block users from using their corporate credentials on sites that do not belong to the corporate domain.
- AI Site Access Control: The solution shall have the option to block access to artificial intelligence sites.
- Safe Search Enforcement: The solution shall enforce "Safe Searching" features when utilizing Google, Bing, and Yahoo search engines.

Data Loss Prevention (DLP)

- Cloud DLP Protection: The solution should provide upload and download protection to and from cloud services.
- Data Type Flexibility: The solution should provide predefined data types to be used, as well as the option to customize data types to be allowed/blocked.
- Policy based on Data Formats: The solution should support creating policies based on specific data formats to be allowed/blocked.
- AI Platform Text Scanning: The solution should provide a text scan on AI platforms to prevent data leakage to AI databases.
- DLP Visibility: The solution should provide complete visibility of DLP insights and events.
- Endpoint Data Control: The solution should provide clipboard control, copy/paste restrictions, print restrictions, and save restrictions.
- Data Type Grouping: The solution should allow data type grouping to improve user experience in setting policies.
- SaaS discovery, misconfiguration detection and automated response

Compliance, Policy, & Posture

- OEM Certifications: The OEM should comply with global certifications like SOC2, Type 2, GDPR, ISO, etc.
- Granular Policy Creation: Policies should be based on users, groups, IP objects, FQDNs, ports, and services.
- Posture-Based Policies: The solution should be able to create policies or posture profiling based on different categories of users.
- Device Inventory & Visibility: The solution shall provide detailed device inventory capabilities, including visibility of connected devices, posture status, serial number, location, and online/offline status.
- Windows Posture Checks: The solution should support posture check options for Windows OS: OS version, certificate presence, running processes, running

antivirus, file existence, disk encryption status, registry key presence, AD association, and Windows Security Center firewall/AV registration status.

- macOS Posture Checks: The solution should support posture check options for macOS: OS version, certificate presence, running processes, running antivirus, file existence, and disk encryption status.
- Regular Posture Assessment: The solution should have a feature to perform regular posture checks (e.g., every 20-30 minutes).
- Full API Access: The OEM shall include full API access to all SASE functions without requiring paid API consumption models.

Threat Intelligence Integration

- Unified Threat Intelligence: The solution shall use one shared threat intelligence database across SASE, EDR, Sandbox, and other components, with unified indicator sharing or native integration with similar threat intelligence technology.

ANNEXURE-1

Technical Bid Format

Please ensure that every requirement has been answered in the technical bid submission format. Failure to do so might lead to a rejection of the bid. The technical bids submitted shall cover the following sections:

Sr. No	Section	Instruction for Response
1	Company Profile	Describe about yourself and your experience in the relevant field.
2	Meeting the Eligibility criteria.	Attach all the requisite Documents in meeting the eligibility criteria as per **Annex-2**& **Annex-4**
3	Understanding of Project Scope	Describe your understanding of the scope of work.
4	Delivery Plan	Share a Detailed Delivery Plan in meeting the timely delivery of scope of work.
5	Resources and responsibilities expected from HPGCL	List out the Resources and responsibilities as expected from HPGCL.

ANNEXURE-2

Meeting the Eligibility criteria.

SN	Qualifying Criteria	Document Attached
a)	The bidder eligible for participating in the bidding process shall be a legal Business Entity	Yes/No Page No. _____ of Bid
b)	The bidder should have Minimum Average Annual Turnover of INR4.98 Crore of last three financial years (i.e. year 2022-23, year 2023-24 & year 2024-25). The net profit of the company shall be positive each of the last three financial years.	Yes/No Page No. _____ of Bid
c)	Bidder must have successfully executed 19.93 Crore "or" two works of 12.46 Crore "or" three works of 9.96 Crore for similar Systems for similar Systems during last 5 financial years for similar work viz any kind of Cyber Infrastructure, Firewalls, Networking equipment's etc.	Yes/No Page No. _____ of Bid
d)	The bidder should have a registered number of Income Tax / PAN number GSTIN	Yes/No Page No. _____ of Bid
e)	The Bidder should not be debarred/blacklisted by any Government / PSU in India as on date of submission of bid.	Yes/No Page No. _____ of Bid
f)	The Bidder should have authorization from the Original Equipment Manufacturer (OEM) for the equipment's i.e.EDR, Anti-APT/Sandbox etc.	Yes/No Page No. _____ of Bid
g)	The Bidder shall submit technical compliance vetted by OEM for under Section 9 i.e Technical Specifications	Yes/No
h)	Tender Document signed and stamped on each page as a mark of acceptance.	Yes/No
i)	Payment of Tender Document and EMD	Yes/No Page No. _____ of Bid
j)	Any other document	Yes/No Page No. _____ of Bid

ANNEXURE-3

Cover Letter Format

Bid Reference No.:

From:

Bidders Name and Address:
Person to Be Contacted:
Designation:
Telephone & Mobile No(s):
Fax No.:

To:

XEN/IT& ERP
Haryana Power Generation Corporation Limited
Room No. 307, Urja Bhawan, C-7, Sector-6, Panchkula.
Haryana – 134109, India.
Ph: 0172-5022416

Subject: **Submission of Technical Bid for Supply, installation & commissioning of Cyber Security Solution including hardware, comprehensive warranty, licenses and premium support and onsite engineer for a period of 5 years.**

We, the undersigned bidder, having read and examined in detail the specifications and the NIT in respect of the Scope of Work do hereby propose to provide services as specified in the NIT. We also declare that:

1. The prices mentioned in our Bid are in accordance with the terms as specified in NIT. The prices and other terms and conditions of this Bid are valid for the period of 120days from the date of opening of financial bid.
2. We declare that all the services/works shall be performed strictly in accordance with the NIT No. _____ dated [date].
3. We declare that our bid prices are for the entire scope of the work as specified in the NIT. These prices have been submitted in the Financial Bid.
4. We further declare that the prices stated in our Bid are in accordance with NIT &will not be subject to escalation for any reason whatsoever within the period of project. A Bid submitted with an adjustable price quotation or conditional Bid may be rejected as non-responsive.
5. Our Proposal is binding upon us and subject to the modifications resulting from contract negotiations

This is to further certify that all the information contained in the Bid is to the best of our knowledge and the bids submitted are completely unconditional.

Thanking you,

Yours faithfully,
(Signature)

Name of Authority Signatory:
Designation& Seal
Date:
Place:
Business Address:

Annexure-4

Certificate Regarding no Deviations
(On letter head of the Bidder)

Bid Reference No.:
To:

XEN/IT& ERP
Haryana Power Generation Corporation Limited
Room No. 307, Urja Bhawan, C-7, Sector-6, Panchkula.
Haryana – 134109, India.
Ph: 0172-5022416

Subject: e-Tender NIT for Supply, installation & commissioning of Cyber Security Solution including hardware, comprehensive warranty, licenses and premium support and onsite engineer for a period of 5 years.

Dear Sir,

We hereby certify that we have gone through all terms and conditions of your e-TENDER No. ..... dated ..... and confirm that the bid submitted by us is in total compliance of the terms of bid documents and no deviations whatsoever are incorporated in our bid.

We further undertake that the entire work shall be performed as per the terms of the above bid documents.

Date :
Place:

Yours faithfully,

(Signature)

Name of Authority Signatory:
Designation& Seal