INQUIRY NO. AEGCL/MD/IT/TECH/CYBER_SECURITY/PROCUREMENT/06 Dated:04/08/2023

Invitation of quotation
for
Supply and Installation of End Point Security (Antivirus) solution with Cloud Based Centralized Management Console at Assam Electricity Grid Corporation Limited Offices.

Inquiry No.	:	AEGCL/MD/IT/TECH/CYBER_SECURITY/PROCUREMENT/06
Submission Start Date	:	Date: 05/08/2023, 11:00 AM
Last Date of Submission	:	Date: 14/08/2023, 11:00 AM

Backbone of Assam Power Network

Assam Electricity Grid Corporation Limited
1st Floor, Bijulee Bhawan, Paltan Bazar, Guwahati-01.
Website: www.aegcl.co.in
Email: infosec@aegcl.co.in

Fees-Rs 1000/-
EMD: Rs 19860/-

Quotation Inviting Authority

Chief General Manager (T&C and Comm),
Assam Electricity Grid Corporation Limited.

A. Invitation of sealed-quotation

Quotations are hereby invited by the undersigned on behalf of the Managing Director, AEGCL, Bijulee Bhawan, Paltan Bazar, Guwahati-01 for Supply and Installation of End Point Security (Antivirus Solution) with Cloud Based Centralized Management Console with 1-year license along with maintenances & support for the Corporation as per terms & conditions mentioned below. The filled quotations along with all the required document must be submitted to AEGCL HQ on or before 14/082023, 11:00 AM. The bids submitted must be in 2 ways envelop process.

B. Terms & Conditions:

1. The quotations received after this deadline & unsealed shall not be entertained under any circumstances whatsoever. In case of website issue this Corporation will not be responsible. **The offer Submitted Fax/Email/Courier etc shall not be considered and no correspondence will be entertained in this matter.**

2. Quotations must be in the enclosed prescribed Performa on the letter head of the firm duly signed by the Proprietor/ Partner/ Director or their authorized representative, in case of signing of quotation by the authorized representative letter of authorization must be attached with the quotation.

3. Rates must be quoted in **Indian rupees** and as per the format specified taxes extra if any must be written separately.

4. Rates must be quoted FOR basis (including Freight charges, installation, other charges etc.)

5. The rates quoted must be valid for 180 days minimum from the date of opening of the quotation and silence of any tendered on this issue shall be treated as agreed with this condition.

6. Becoming L1 will not be the criteria for awarding of purchase order unless the rates are reasonable & justified.

7. RTGS/NEFT details need to be furnished by the supplier with the quotation on the letter head of supplier/firm/agency.

8. The firm/agency may satisfy the following conditions and attach self-attested copy of the same with the quotation:

    a. Firm shall be registered.

    b. The firm shall have valid GST No.

    c. Documentary proof certificate (certified by CA/CMA) of an Annual Turnover More Than Rs 10 Lakhs.

9. Fees Rs 1000/- (Non-Refundable) in the form DD only or through online banking etc and EMD- Rs. 19860/- (Refundable) in a form of DD/BC/Call Deposit only in favor of AEGCL shall be submitted in case of offline and for e-offer EMD shall be submitted online. Failing of this led to rejection of your offers.

10. The quotationer should be either OEM (Original Equipment Manufacturer) or a distributor, a dealers or a reseller. Quotationer shall submit authorization letter from the OEM in this regard.

11. Necessary arrangements should be provided to make the engineers of AEGCL, familiar with products, through induction training, workshop etc. AEGCL shall only provide the training hall. All other cost etc. to be provided by the quotationers.

12. Submission of Authorization certificate from the OEM as per Annexure-V

13. Submission of Bank Details as per Annexure-IV and Compliance report w.r.t. Annexure-III.

14. MSME registered bidder under IT/software related category is exempted from submission of EMD only.

15. Copy of PAN Card along with copies of IT Returns of the firm for the preceding three years

16. Copies of Balance Sheets and audited financial statements of the firm for the preceding three years including the year 2022-2023

17. At least One Copy of previous supply orders (during the last 3 years from the date of publishing of NIT) to Government departments or reputed public institutions from the OEM.

18. AEGCL reserves the right to cancel the tender at any point of time without assigning any reason.

19. All other terms and conditions which are not mentioned here may please be refer to AEGCLs' General Conditions of Supply and Erection 2009. For details visit https://www.aegcl.co.in/rules-regulations/

C. OTHER NECESSARY TERMS AND CONDITIONS

1. Performance Security: The successful bidder will be required to furnish Performance Security of 10% of the value of the total contract amount in the form of Demand Draft/Pay Order in favor of MD, AEGCL at Guwahati within 10 days of receipt of the supply order. The Performance Security would be retained by the AEGCL till satisfactory completion of supply, installation and warranty obligations. The Performance Security shall remain valid till 60 (sixty) days of the completion of the contract period including warranty obligations.

2. The number of the users for the End Point Security with Centralized Management Console (Cloud based) is initially fixed at 550 nos. However, the number of users may increase depending on the requirement of the Commission and the successful bidder must provide the same at the same rate. Payment will be made on the number of licenses ordered.

3. AEGCL intends to keeps the solution deployed for 3 years and same may be further extended. OEM/Distributor/Authorized reseller shall provide an undertaking stating they will extend their service at the same rate without any condition. However, payment shall be made yearly basis on the actual nos. of End Point Security licenses deployed based on mutual understanding.

4. AEGCL shall be at liberty to terminate the contract giving one-month advance notice.

5. The OEM must have at least five (5) years of experience in developing IT security related products and the product to be supplied by the bidder of the respective OEM should be installed in at least three (3) Govt. Department or reputed public institution with at least 100 user licenses with a support for a period of at least 1 year. In this regard, relevant supporting documents needs to be submitted.

6. The bidder (OEM/supplier/distributer etc.) shall have at least three (3) years of experience in supply and installation of IT security systems in any Govt. Department or reputed Public Institution. In this regard, the bidder shall submit a copy of previous supply orders in support of his/her experience.

7. The proposed End Point Security solution should be in Gartner's Magic Quadrant for End Point Security Solution. Proof of the same must be attached along with tender papers.

8. Taxes shall be quoted separately along with per unit cost.

9. Risk Purchase Clause: If the firm after submission of bid and due acceptance of the same i.e. after the placement of order fails to abide by the terms and conditions of the tender document, AEGCL will have the right to forfeit the EMD, invoke the performance security deposited by the firm and procure the item from other firm at the risk and consequence of the firm. The cost difference between the alternative arrangement and firm's bid value will be recovered from the firm along with other incidental charges including custom duties, taxes, freight and insurance etc. In case AEGCL is forced to procure the material through alternative source and if the cost is lower, no benefit on this account would be passed on to the firm.

10. Delivery, installation and commissioning: - Within 60 days of issue of supply order.

11. Endpoint Locations:

    AEGCL's offices where proposed End Point Security solution are to be installed:

Sl. No.	**Office Address**	**No. of PC/Laptop**
	Lower Assam Region	
1.	Head Office, Bijulee Bhawan, Guwahati	Server-2 nos. Laptop/Desktop – 165 nos.
2.	Narengi LA T&T Circle (08), Transmission Division(05), 132/33 Kv Narengi (01), Narengi MRT (05),LA T&T Zone (03) T&C And Communication (07), P&D (17), GM LAZ Narengi (04)	Laptop/Desktop – 50 nos.
3.	Kahilipara Kahilipara Division (08), SLDC (37), Communication Division (06), MRT Division (05)	Laptop/Desktop – 56 nos.
4.	Rangia 220 Kv Rangia GSS (04), 132 Kv Rangia GSS (02)	Laptop/Desktop – 06 nos.
5.	220 Kv Sarusajai GSS	Laptop/Desktop – 06 nos.
6.	Bongaigaon T&T Circle	Laptop/Desktop – 03 nos.
7.	Dhaligaon 132 KV AGM Dhaligaon (06), AGM Maintenance (01), T&C Division (06)	Laptop/Desktop – 13 nos.
8.	220 KV Salakati GSS	Laptop/Desktop – 07 nos.
9.	T&T Technical Mirza	Laptop/Desktop – 05 nos.
10.	Maintenance Subdivision AGIA	Laptop/Desktop – 02 nos.
11.	132 KV Baghjap	Laptop/Desktop – 01 nos.
12.	132 KV Sishugram GSS	Laptop/Desktop – 01 nos.
13.	220 KV GIS Sonapur	Laptop/Desktop – 01 nos.

14.	132 KV Chandrapur GSS	Laptop/Desktop – 01 nos.
15.	132 KV Capital (Dispur) GSS	Laptop/Desktop – 01 nos.
16.	132 KV Kamakhya GIS	Laptop/Desktop – 01 nos.
17.	132 KV Kamalpur GSS	Laptop/Desktop – 01 nos.
18.	132 KV Sipajhar GSS	Laptop/Desktop – 01 nos.
19.	132 KV Nalbari GSS	Laptop/Desktop – 01 nos.
20.	220 KV GIS Jawaharnagar	Laptop/Desktop – 01 nos.
21.	132 KV Joyma GSS	Laptop/Desktop – 01 nos.
22.	132 KV Barnagar GSS	Laptop/Desktop – 01 nos.
23.	132 KV Kokrajhar GSS	Laptop/Desktop – 01 nos.
24.	132 KV Gauripur GSS	Laptop/Desktop – 01 nos.
25.	132 KV Bilasipara GSS	Laptop/Desktop – 01 nos.
26.	132 KV Azara	Laptop/Desktop – 01 nos.
27.	Kukurmara AGM T&C And Comm. Kukurmara (04) 400 KV Kukurmara GSS (05)	Laptop/Desktop – 09 nos.
28.	220 KV Boko GSS	Laptop/Desktop – 02 nos.
29.	132 KV APM Jogighopa	Laptop/Desktop – 01 nos.
30.	132 Matia GSS	Laptop/Desktop – 01 nos.
31.	AGM Goalpara Transmission Division	Laptop/Desktop – 03 nos.
32.	132 KV Barpeta GSS	Laptop/Desktop – 01 nos.
33.	132 KV Tangla GSS	Laptop/Desktop – 01 nos.
Central Assam Region		
34	Tezpur AGM T&C And Comm (05), DGM T&T Circle (09)	Laptop/Desktop – 14 nos.
35.	Nagaon AGM T&C Samaguri (04), Communication Division Samaguri (05), DGM T&C And Comm Samaguri (03), GM CAZ T&T Zone Nagaon (04), T&T Division Samaguri (07), AGM 220 KV Samaguri GSS(07)	Laptop/Desktop – 30 nos.
36.	Depota	Laptop/Desktop – 08 nos.

	AGM Depota EHV GSS (06), MSD Depota (02)	
37.	Silchar AGM T&C And Comm (02), DGM T&T Circle (08), AGM T&T Division Sllchar (04)	Laptop/Desktop – 14 nos.
38.	Panchgram AGM Panchgram Division (05), 132 KV Hailakandi GSS (01), LMSD Panchgram (01)	Laptop/Desktop – 07 nos.
39.	132 KV Umrangso GSS	Laptop/Desktop – 01 nos.
40.	132 KV Khaloigaon GSS	Laptop/Desktop – 01 nos.
41.	220 KV Sonabil GSS	Laptop/Desktop – 01 nos.
42.	132 KV Ghoramari GSS	Laptop/Desktop – 01 nos.
43.	132 KV Rowta GSS	Laptop/Desktop – 02 nos.
44.	132 KV Dhekiajuli GSS	Laptop/Desktop – 01 nos.
45.	132 KV Sankardevnagar GSS	Laptop/Desktop – 01 nos.
46.	132 KV Srikona GSS	Laptop/Desktop – 01 nos.
47.	132 KV Pailapool GSS	Laptop/Desktop – 01 nos.
48.	132 KV Haflong GSS	Laptop/Desktop – 03 nos.
49.	132 KV Hailakandi GSS	Laptop/Desktop – 01 nos.
50.	132 KV Dullavcherra GSS	Laptop/Desktop – 01 nos.
51.	132 KV Karimganj GSS	Laptop/Desktop – 02 nos.
UPPER ASSAM REGION		
52.	Dibrugarh 132 KV Dibrugarh GSS (05), DGM T&C (04), AGM T&C (03), DGM T&T Circle (06), GM UAZ T&T Zone Dibrugarh (04)	Laptop/Desktop – 22 nos.
53.	220 KV Tinsukia GSS	Laptop/Desktop – 05 nos.
54.	Jorhat MRT Garmur (07), Garmur GSS Jorhat (01), DGM T&T Circle (06), AGM UA Communication (09), T&T Division (04), Jorhat West GSS (01)	Laptop/Desktop – 28 nos.
55.	AGM 132 KV Gargaon Nazira	Laptop/Desktop – 09 nos.
56.	AGM 220 KV Mariani GSS	Laptop/Desktop – 08 nos.
57.	132 KV Golaghat GSS	Laptop/Desktop – 02 nos.
58.	T&T Division	Laptop/Desktop – 05 nos.
59.	North Lakhimpur	Laptop/Desktop – 13 nos.

	AGM 132 KV Nalkatta GSS (04), AGM T&C Division North Lakhimpur (03), DGM T&T Circle (06)	
60.	132 KV Chapakhowa GSS	Laptop/Desktop – 01 nos.
61.	132 KV Sonari GSS	Laptop/Desktop – 02 nos.
62.	132 KV LTPS GSS	Laptop/Desktop – 01 nos.
63.	132 KV Moran GSS	Laptop/Desktop – 01 nos.
64.	132 KV Bordubi GSS	Laptop/Desktop – 01 nos.
65.	132 KV Margherita GSS	Laptop/Desktop – 01 nos.
66.	132 KV Rupai GSS	Laptop/Desktop – 01 nos.
67.	132 KV Teok GSS	Laptop/Desktop – 01 nos.
68.	220 KV Namrup GSS	Laptop/Desktop – 01 nos.
69.	132 KV Bokajan GSS	Laptop/Desktop – 01 nos.
70.	132 KV Bokakhat GSS	Laptop/Desktop – 02 nos.
71.	132 KV Sarupathar GSS	Laptop/Desktop – 01 nos.
72.	132 KV Diphu GSS	Laptop/Desktop – 01 nos.
73.	132 KV Majuli GSS	Laptop/Desktop – 01 nos.
74.	132 KV Betbari (Sibsagar) GSS	Laptop/Desktop – 01 nos.
75.	132 KV Behiating GSS	Laptop/Desktop – 01 nos.
76.	132 KV Gohpur GSS	Laptop/Desktop – 01 nos.
	Total	Laptop/Desktop – 550 nos.

It will be successful bidder's responsibility to install the solution in the PC/Laptop in the office location. However AEGCL will extend support in installing the End Point Software in the locations through the resources available at Circle Offices of AEGCL.

12. Arbitration: Any dispute or difference whatsoever arising between AEGCL and the firm out of or relating to the conclusion, meaning and operation or effect of the contract or the breach thereof shall be settled by the Arbitrator to be appointed by AEGCL in accordance with the provisions of Arbitration and Conciliation Act, 1996 and the award in pursuance thereof shall be binding on AEGCL and the firm. The venue of Arbitration shall be at Guwahati.

13. Jurisdiction: Subject to the arbitration herein above provided, any suit or proceedings to enforce the right of either of the parties hereto the contract shall be instituted in and tried only by the courts in Guwahati and by no other court, and both the parties hereto hereby expressly agree to submit to the jurisdiction of such court.

D. Payment Terms:

1. 90% payment would be released after successful supply and installation of the antivirus software in all the servers & desktops/laptops installed in the AEGCL.

2. The remaining 10% payment would be released after 365 days on successful installation.

3. The End Point Security Software with Cloud based Centralized Management Console shall initially be for 550 users. The contract shall have license initially for one year. The product must have the facility of being renewed every year for 3(three) years or more with regular updates & onsite support. It shall be procured only for the number of user/licenses during the currency of the contract. AEGCL shall pay the cost of additional user/license as per the approved rates only. No other charges shall be paid for this.

4. Force Majeure: The firm shall not be responsible for any failure to perform due to causes beyond its reasonable control including, but not limited to acts of God, war, riots, embargoes, strikes, lockouts, act of any Government authority, delay in obtaining licenses or rejection of applications under the statutes, power failure, accidents or disruption or operations arising from causes not attributable to any mala fide acts of firm, fire or floods.

5. AEGCL reserves the right to accept or reject all or any of the bids without assigning any reasons. The decision of the MD, AEGCL would be final and binding.

6. Hypothetical and conditional bids will not be entertained.

7. The bids shall be valid for 180 days from the date of opening of technical bids.

8. The tender notice is also available on AEGCL's website: www.aegcl.co.in

9. **The firm should not be black listed by any Govt. Agency/Dept.**

   Quotations qualified by such vague and indefinite expressions such as “subject to prior confirmation”, “subject to immediate acceptance” etc. will be treated as vague offers and rejected accordingly. Any conditional quotation shall be rejected summarily.

10. **Delivery Period** – within 60 days from Purchase order.

11. **Liquidated Damage: -** If the supplier fails to deliver the material on or before the stipulated date, then a penalty at the rate of 0.5 % per week of the total order value shall be levied subject to maximum of 10% of the total order value.

12. **Disputes: -**In the event of any dispute or disagreement arising between the contractors and any other department of AEGCL, Bijulee Bhawan, Paltan Bazar, Guwahati-01 with regards to the interpretation of “Terms & Conditions” of this inquiry, the same shall be referred to the Managing Director, AEGCL, Bijulee Bhawan, Paltan Bazar, Guwahati-01 whose decision will be final and binding upon the contractor.

13. AEGCL reserves the right to increase or decrease quantity and / or amount of work. Decision of Quantity of material in the AEGCL will be final in this regard.

14. AEGCL reserves the right to reject any quotation or part or the whole of inviting quotation process without assigning any reason. Decision of the AEGCL will be final in this regard.

E. Special Terms & Conditions:

1. **Bidder must quote the product as per specification provided in Annexure 1.**

2. **Catalogue must be attached with quotation for technical evaluation.**

3. **The supplier may be asked to arrange demonstration of their product for which rates have been quoted, to the AEGCL, if required. The expenditure incurred for demonstrating the items will be borne by the supplier.**

Encl.: Annexure 1 & 2 (Specification) Annexure 3 (Format of price bid)

The below-mentioned Financial Proposal/Commercial bid format is provided and quote their offer/rates in the permitted column and submitted the same in the commercial bid. **Bidder shall not tamper/modify downloaded price bid template in any manner.** In case if the same is found to be tampered/modified in any manner, tender will be completely rejected and EMD would be forfeited and tenderer is liable to be banned from doing business with AEGCL.

Financial Bid

S.N	Name of the Item	QTY	Per unit cost (in Rs.)	Taxes, if any	Total per unit cost
1	End Point Security Software for 550 users with Cloud based Centralized Management Console (License for one year) with regular updates & onsite support	1	**To be filled only in BoQ format**		

* L-1 will be determined on the basis of unit per unit cost plus taxes as applicable

Annexure-I Specification:

Technical Specification for Antivirus Software		Compliance Yes/No
S. No	**End Point Security Software to protect Desktops/Laptop & Servers with following functionality for 550 users with Cloud Based Centralized Management Console**	
1	End Point Security solution Should have a Cloud based Centralized Management Console for both Servers & desktop/laptop	
2	The End Point Security solution should provide protection for desktops & servers of all the attacks originating from places inside/outside of the network due to virus and/or other malicious programming code.	
3	The End Point Security solution should Support Multi-Platform operating system (Windows, Mac & Linux) and the same should be managed from a single cloud based Centralized Management console.	
4	Solution should have an application-based console	
5	End Point Security Solution should have single, Configurable Installation with centralized configuration *&* policy management.	
6	Automatic update of End Point Security from Original Software Developer (OSD)/Original Equipment Manufacturer (OEM) & the client should get update from the local Server If updating from the Primary Server fails for any reason (such as the user being off the network) an attempt should be made to contact the Secondary Server (i.e. OSD/OEM).	
7	End Point Security should have centralized scanning of all network Systems	
8	Administrator should have flexibility to schedule Scan and update at the endpoints from central Server.	
9	End Point Security should be able to capture Viruses, Trojans, Worms, Spyware and Malware, adware and Potentially Unwanted Application (PUA) from single agent.	
10	End Point Security Should have Host Intrusion Prevention System (HIPS)technology which works in 4 Layers to provide zero-day protection without the need for updates (Unknown Virus Detection & Repair).	
11	End Point Security should have run time detection technology i.e., behavioral & Heuristic scanning to protect from unknown viruses and buffer overflow protection integrated with AV scan engine for protection from threats/exploits that uses buffer overflow	
12	End Point Security Software must have the capability to clean, Quarantine or delete Viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms	
13	End Point Security OSD/OEM should provide definitions with incremental updates. Should support daily update for definition files. Size of daily update should be extremely small in size (typically between 25 and 500kb in size)	
14	Administrator Should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.	
15	Administrator should be able to lock down all End Point Security configurations at the desktop & User should be prevented from being able to uninstall the anti-virus software.	
16	Administrator must be able to distribute new and update End Point Security software, virus definitions and Policies automatically to clients and servers from a central	
17	End Point Security should provide centralized event logging to locate and cure virus	
18	Alerts on virus activity should be passed on to administrator	
19	End Point Security Should have Personnel Firewall (Client Firewall) with location awareness feature and it should block unsolicited inbound traffic, control outbound traffic, and apply policy rules based on traffic, ports, applications, and locations.	

20	End Point Security should have a Live web protection module Integrated into existing endpoint agent with no endpoint configuration required to Blocks URLs that are hosting malware and Should Support all major browsers - IE, Firefox, Safari, Opera, Chrome etc.	
21	Solution Updates should not be more than 30-50Kb with multiple updates to Reduce Minimum impact on Bandwidth.	
22	Solution must support Device Blocking and Exceptions with Vendor and Model (Device ID), with the option of Block/Read/Allow.	
23	OEM should have Standalone End Point Security scanner in a Bootable format for all Operating Systems.	
24	OSD/OEM Should have 24x7 toll free Global Technical Support.	
25	End Point Security solution should be a Gartner leader for one year or more during the last five years.	

Annexure-II Specification: (Special Condition)

Sl No.	Technical Specification (Endpoint Security – Cloud Based)	Compliance
1	Must offer comprehensive endpoint security by providing virus protection, spyware, rootkits, bots, grayware, adware, mal ware and other computer borne threats or mixed threat attacks or any emerging cyber-attacks or zero-day attack protection.	
2	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files) through a fully-automated process.	
3	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	
4	Must include capabilities for detecting and removing rootkits	
5	Must provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution	
6	Must have capabilities to restore spyware/grayware if the spyware/grayware is deemed safe	
7	Must have Assessment mode to allow first to evaluate whether spyware/grayware/ malware is legitimate and then take action based on the evaluation	
8	Solution must provide these capabilities in a single agent: antimalware, application control, virtual patching, host firewall, URL reputation-based blocking, machine learning, behaviour monitoring, DLP, USB blocking, ransomware protection.	
9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to: a) Terminating all known virus processes and threads in memory b) Repairing the registry c) Deleting any drop files created by viruses d) Removing any Microsoft Windows services created by viruses e) Restoring all files damaged by viruses f) Includes Clean-up for Spyware, Adware etc.	
10	Must be capable of cleaning viruses/malware even without the availability of virus clean- up components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether.	
11	Must provide suitable Outbreak Prevention Solution either through limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected customers or equivalent features in case there is an outbreak.	
12	Behaviour Monitoring: a) Must have behaviour monitoring to restrict system behaviour, keeping security related processes always up and running b) Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent	
13	Must provide Real-time lock down of customer configuration allow or prevent users from changing settings or unloading/uninstalling the software	
14	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	
15	CPU/memory (physical or virtual) usage performance control during scanning: a) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer b) Adjusts the scanning speed. c) The CPU usage level is High, Medium or Low d) Actual CPU consumption exceeds a certain threshold	
16	Should have a manual outbreak prevention feature that allows administrators to configure USB ports control (Open/Close for use) and deny writes to files and folders manually	

17	Should have the capability to assign a customer the privilege to act as an update/master relay agent for rest of the agents in the network	
18	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
19	Shall be able to scan only those file types which are potential virus carriers (based on true file type)	
20	Should be able to detect files packed using real-time compression algorithms as executable files.	
21	Shall be able to scan Object Linking and Embedding (OLE) File	
22	Must provide Web threat protection by the following ways: a) Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings b) Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location c) Must have the capabilities to define Approved URLs to bypass Web Reputation policies d) Must provide real-time protection by referencing online database with millions of rated Web domains e) Configure Web reputation policies and assign them to individual, several, or all end users machine.	
23	Must provide File reputation service a) Must be able to check the reputation of the files hosted in the internet b) Must be able check the reputation of the files in webmail attachments c) Must be able to check the reputation of files residing in the computer	
24	Must protect endpoints on the network from high performance network virus, & do scanning and elimination	
25	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users and provide full disk encryption.	
26	Must have smart feedback to enable feedback from the customer agents to the threat research Centres of the vendor.	
27	Uses any alternate method other than the conventional pattern-based scanning with the following features: a) Provides fast, real-time security status lookup capabilities in the cloud b) Reduces the overall time it takes to deliver protection against emerging threats c) Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints d) Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.	
28	Should be able to deploy the Customer software using the following mechanisms: a) Customer installation Package (Executable & Microsoft Installer (MSI) Package Format), should support silent installer, unmanaged customers, specific installer for servers b) Web install page c) Login Script Setup d) Remote installation e) From a customer disk image	
29	Must provide a secure Web-based management console to give administrators transparent access on the network	
30	The management server should be able to download updates from different source if required.	
31	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.	
32	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console	

33	Should have role-based administration with active directory integration a) To create custom role type b) To add users to a predefined role or to a custom role	
34	Should have integration with the Active directory 2008/2012 or higher	
35	Shall support grouping of customers into domains for easier administration & Endpoint security solution should provide vulnerability protection & CVE number visibility against vulnerability.	
36	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)	
37	Must be capable of uninstalling and replacing existing customer antivirus software and to ensure unavailability of any residual part of the software.	
38	Security Compliance should leverage Microsoft Active Directory services to determine the security status of the computers in the network	
39	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from customer IPS, customer firewall, and/or network virus logs exceed certain thresholds, signalling a possible attack.	
40	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack	
41	Virus definition files should be lighter so that same can be transmitted to remote locations having minimum of 64kbps link or the update pattern size should be less than 200Kb	
42	System should be configured with the option that endpoints can get updated directly from internet or from local security server. This option can be used with flexibility to allow end point to get update from internet or block to stop update from internet.	
43	In case of bot infection, bot removal tools also to be facilitated to clean the infected machine and solution should have the option of the endpoint vulnerability shielding in the network.	
44	The solution should have latest machine learning technology in built from day one and solution should have ransomware protection in built.	
45	Solution must be a leader as per latest report from Gartner/Forrester for Endpoint Protection Platform.	
46	The Solution must support both IPV4 & IPV6	

ANNEXURE-III

Tender for Supply and Installation of End Point Security (Antivirus Solution) at
Assam Electricity Grid Corporation Limited End Point Security (Antivirus Solution)

We_____

_____(Name and Address of the firm) have in response to your NIT _____dated_____submitted a technical and financial bid for supply of Antivirus Software. As required under the NIT, we hereby certify as under: -

1. That all the terms and conditions of the tender are acceptable to us.
2. That the Antivirus Software quoted by us in response to this tender is strictly as per the specifications prescribed in Annexure-I of the tender document.
3. That I/We have not been penalized or convicted for concealment of income/wealth during the immediately preceding three years.

(Authorized Signatory)
Name and Address of the Firm/Bidder

ANNEXURE-IV

Date__	**(Name)_____**
Place	**Name of Firm/Company/Agency_**
	GSTIN No.: ___
	Bank Name:- _
	Bank Account No.: ____
	IFSC Code:- __
	Branch Name:
	Phone No._____
	Email:
	(Signature of Authorized Person) _____
	Seal:__

Annexure-V- Manufacturer's Authorization

[***The Bidder, in pursuant to ECQ Clause 2.1.1 (if applicable) shall require the Manufacturer to fill in this Form in accordance with the instructions indicated. This letter of authorization should be signed by a person with the proper authority to sign documents that are binding on the Manufacturer. Please refer to notes at bottom]***

(Manufacturer's Letterhead)

Date: [***insert date (as day, month and year) of Bid Submission***]

Bid No.: [***insert number of bidding process***]

To: [Insert: full name of Purchaser]

WE *[insert: **name of Manufacturer**]* who are established and reputable manufacturers of *[insert: **name and/or description of the Goods/Software/Service**]* having production/registered facilities/office at *[insert: **address of factory/registered office**]* do hereby authorize *[insert: **name & address of Bidder**]* (hereinafter, the "Bidder") to submit a bid the purpose of which is to provide the following goods/software/service, manufactured/produced by us, and to subsequently negotiate and sign the Contract:

1. ----------
2. ----------

We hereby extend our full guarantee and warranty in accordance with this bid, for the above specified Goods/software/service supporting the Supply of specified Goods/Software/service and fulfilling the Related Services by the Bidder against this Bidding Documents, and duly authorize said Bidder to act on our behalf in fulfilling these guarantee and warranty obligations. We also hereby declare that, we will furnish the Performance Security in accordance with **Clause C 1 in bid .**Further, we also hereby declare that we and ……., *[insert: **name of the Bidder**]* have entered into a formal relationship in which, during the duration of the Contract (**including related services and warranty / defects liability**) we, the Manufacturer or Producer, will make our technical and engineering staff fully available to the technical and engineering staff of the successful Bidder to assist that Bidder, on a reasonable and best effort basis, in the performance of all its obligations to the Purchaser under the Contract.

For and on behalf of the Manufacturer

Signed: _____

Date: _____