भाकृअनुप - राष्ट्रीय कृषि अनुसंधान प्रबंध अकादमी
राजेन्द्रनगर, हैदराबाद-५०००३०, तेलंगाणा, भारत
ICAR-National Academy of Agricultural Research Management
(ISO 9001:2015 Certified)
Rajendranagar, Hyderabad-500030, Telangana, India
Phones: (040) 2458 1322; Fax: (040) 2401 5912; https://naarm.org.in

F.No.5-435/2019-20/Anti-Virus/PS Dated: 12th September, 2022

NOTICE INVITING TENDER FOR
Supply of Enterprise Antivirus Software (Client server) with Endpoint Detection and Response to ICAR-NAARM

ICAR-NAARM is a premier publicly funded Training and Research Management Organization under ICAR, DARE, Ministry of Agriculture & Farmers Welfare, Government of India. The Director, ICAR-NAARM invites Tenders from the authorized suppliers / Dealers / OEM to supply Enterprise Antivirus software to ICAR-NAARM. The bidders are requested to submit the Tenders online **on GeM Portal.** The summary of requirement is as under.

The Director, ICAR - NAARM reserves the right to reject any tender without assigning any reason thereof. Tenders are to be submitted online on GeM Portal**.** A brief detail of tender is given in the following format.

S. no.	Item Description	Quantity	Specification as per
1.	Enterprise Antivirus User License	500 Licenses	Schedule -I
2.	Antivirus Software for Servers	3 Licenses	Schedule -II
3.	Enterprise Antivirus User License**	200 Licenses	Schedule -I

***Order may be placed for S.no 3 Licenses any time during the contract period in addition to S.no. 1 and 2 as per the need of academy in a staggered manner and bill be paid as per actual licenses subscribed. There can also be the case that S.no 3 may not be ordered at all.*

Senior Administrative Officer

TERMS AND CONDITIONS:

1.	**Online bids** on GeM are invited for and on behalf of the Director, ICAR – NAARM, from eligible bidders for SUPPLY OF ENTERPRISE ANTIVIRUS SOFTWARE (CLIENT SERVER) WITH ENDPOINT DETECTION AND RESPONSE
2.	All communications must be addressed to the Director, ICAR-NAARM, Rajendranagar, Hyderabad.
3.	**Specification of item:** The detailed specification of the different items is provided in SCHEDULE – I of this tender document.
4.	The **Security Money Deposit** (EMD) is 3% of the total final cost of tender which will be refunded / returned only after satisfactory completion of the contractual obligation. The Security Deposit should be in the form of Demand Draft, Fixed Deposit Receipt or Bank Guarantee from any commercial bank and on which no interest will be paid.
5.	**Eligibility Criteria:** a. Filled **Annexure - A** b. Filled Details as per **Annexure-B** along with Complete tender document duly sealed and signed c. Undertaking as per **Annexure – C on Company Letter Head.** **d. Data Sheet(s) of the product offered in the bid are to be uploaded along with the bid documents. NAARM can match and verify the Data Sheet with the product specifications offered. In case of any unexplained mismatch of technical parameters, the bid is liable for rejection.** **e. Upload Manufacturer authorization: Wherever Authorized Distributors are submitting the bid, Manufacturers Authorization Form (MAF)/Certificate with OEM details such as name, designation, address, e-mail Id and Phone No. required to be furnished along with the bid.** **f. Proof of Offered Product being listed in Gartner Leader/ Gartner Magic Qudrant.** **g. Proof of Experience of 5 Years or more in Antivirus/Cyber Security sector. Supporting documents are to be provided.** **h. Certificate to the effect that Rates offered are those offered to Government/Academic institutions.** **i. Provide Dedicated /Toll Free telephone number of Service & Support of your firm. BIDDER/OEM must have Dedicated/toll Free Telephone No. for Service Support.** **j. Bidder/OEM must provide Escalation Matrix of Telephone Numbers for Service Support.** k. Scanned copy PAN & GSTIN Registration. (all scanned and combined in one pdf) l. The firm should enclose copies of income tax returns for the last 3 years (Financial Year 2017-18, 2018-19, 2019-20)
6.	**Rejection of tenders**: Tenders not complying with any one of the above conditions, are liable to be rejected. No correspondence in this regard will be entertained.
7.	**Rates:** Rates should be quoted in the prescribed Financial BOQ in Indian Rupees only. The rates quoted shall be valid for a minimum period of 180 days (6 months) beyond the date of opening of tenders.

8.	**Contract Period:** The contract will be valid for 3 years (That is the subscription period of the antivirus supplied), which may be extended for further two years, one year at a time subject to satisfactory completion of work orders.
9.	**Delivery Schedule:** The item should be provided within 20 days of issuance of supply order .
10.	**Financial Bid:** The financial bid has to be uploaded on GeM portal as per the format of BOQ uploaded along with the tender. The cost per unit for Sl.No. 3 should not be more than cost per unit of S.N.1
11.	**Liquidated Damages:** As per GeM terms and conditions
12.	If after finalization of the tender, the selected firm expresses its inability provide the printing job work done at the quoted rates, thus failing in fulfilling the stipulated terms and conditions for award of the contract, then the Security Deposit amount is liable to be forfeited in total.
13.	**Payment : Payment will be made as per the terms and conditions of GeM as per the supplied licenses.**
14.	**Taxes / Duties:** If taxes, duties, or any other charges over and above the rates quoted are payable by the Academy, actual / percentage of such taxes / duties / charges should be clearly indicated.
15.	**Acceptance of tender:** Director, ICAR-NAARM reserves the right to accept or reject any of the tenders either in part or in full without assigning any reason thereof.
16.	**Jurisdiction:** All disputes including court proceedings shall be settled within the Hyderabad jurisdiction only.
17.	**No Exemption to startups** has been given as the work is of high value and involves printing of scientific publications.
18.	**SCOPE OF WORK:** The Antivirus software solution need to be installed on to a dedicated server and 1. Configure/ customize the server according to client requirements or client's IT environment. 2. Install client side software on all desktop. 3. First time demonstration of the features/ functioning of software to client's IT staff. 4. Submit commissioning report after completion of work. 5. Provide helpdesk/ support escalation matrix. 6. Creating rules/ policies in antivirus server according to the client's need. 7. It should meet all requirements and 30 specifications as mentioned in Schedule – I of this tender document. 8. Installation, Commissioning, Testing, Configuration, Training (if any - whichever is applicable as per scope of supply) is to be carried out by OEM / OEM Certified resource persons or OEM authorized Reseller only.

(Senior Administrative Officer)

Schedule –I

SPECIFICATIONS OF THE ENTERPRISE ANTIVIRUS CONTRACT (ITEM @ S.NO 1 AND 3):

Sl. No.	Descriptions
1	**Integrated Management**
	Must have a unified console for managing multiple products such as Advanced Endpoint Protection, Email Gateway, Server Security, Mobile Control etc.
	All settings for these products MUST be configured from a Central Dashboard without the need to access additional consoles.
2	**Multi-Platform Management**
	Windows, Mac, and Linux machines must be managed from one management console.
3	**SIEM Integration**
	Must have the capability to extract events and alerts information from the Cloud Dashboard to a local SIEM.
4	**Role Management**
	Must have the capability to allow the separation of estate management to different administrator login.
	Must provide admins the capability to assign predefined administrative roles to users who need access to the Admin Console.
	Must be able to create custom roles and assign the products and access needed.
5	**Microsoft AD Synchronization**
	Must have the capability to only allow outbound synchronization of Users/Groups from the local Active Directory servers.
6	**Microsoft Azure AD Authentication**
	Must have the capability to log in to the Admin Dashboard and Self Service Portal using Azure AD Login
7	**Policies**
	Selected policies should be able to be applied to either users or devices.
	Policies must have the capability to be disabled automatically based on a scheduled time and date.

8	**Enhanced Tamper Protection**
	Must have the capability to prevent local administrative users or malicious processes from disabling the endpoint protection.
	Must have the capability to prevent the following actions on the endpoint protection solution:
	1) Stopping services from the Services UI
	2) Kill services from the Task Manager UI
	3) Change Service Configuration from the Services UI
	4) Stop Services/edit service configuration from the command line
	5) Uninstall
	6) Reinstall
	7) Kill processes from the Task Manager UI (desired)
	8) Delete or modify protected files or folders
	9) Delete or modify protected registry keys
	Must be able to export Tamper Protection passwords in CSV or PDF formats.
9	**Threat Protection**
	Must protect against multiple threats, both known and unknown, and provide a trusted and integrated approach to threat management at the endpoint.
10	**Anti-rootkit Detection**
	Must identify a rootkit when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected.
11	**Suspicious Behavior Detection**
	Must be able to protect against unidentified viruses and suspicious behavior.
12	**Scanning**
	Must provide a scheduled scanner to run depending on the selected frequency or by manually triggering through Windows Explorer to scan the specified directories .
	Must have the capability to scan archives such as zip, cab, etc. which can be enabled via policy settings.
13	**Advanced Deep Learning mechanism**
	Must be able to prevent both known and never-seen-before malware, likewise must be able to block malware before it executes.
14	**Anti-Ransomware Protection**
	Must be able to protect from ransomware that encrypts the master boot record and from attacks that wipe the hard disk.

15	**AMSI Protection**
	Must be able to protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI).
16	**Data Loss Prevention (DLP)**
	Must be able to monitor and restrict the transfer of files containing sensitive data.
17	**Application Control**
	Must have the capability to limit the applications needed for specific user groups.
18	**Web Control**
	Must be able to block risky downloads, protect against data loss, prevent users from accessing web sites that are inappropriate for work, and generate logs of blocked visited sites.
	Must have security options to configure access to ads, uncategorized sites, or dangerous downloads.
19	**Windows Firewall Policy**
	Must be able to monitor and configure Windows Firewall on managed computers and servers using a Windows Firewall policy.
20	**Root Cause Analysis**
	Must have the capability to identify what happened, where a breach originated, what files were impacted, and provides guidance on how to strengthen an organization's security posture
21	**IT Operations**
	Identify unmanaged, guest, and IoT devices
	Why is the office network connection slow? Which application is causing it?
	Look back 30 days for unusual activity on a missing or destroyed device
22	**Threat Hunting**
	Extend investigations to 30 days without bringing a device back online
	Use ATP and IPS detections from the firewall to investigate suspect hosts
	Compare email header information, SHAs, and other IoCs to identify malicious traffic to a domain
23	**Block Applications**
	Must have an option to immediately detect and remove potentially malicious Portable Executable (PE) files from protected computers in the environment.
	Must have an option to block applications using their SHA-256 hash.

24	**On-demand Threat Intelligence**
	Must have an option to 'request intelligence' on suspicious files, which will upload the file to our malware research team for further analysis.
25	**Endpoint Isolation**
	Must have an option to 'manually isolate' protected endpoints from the network while investigating a threat case.
	Must have an option to 'automatically isolate' compromised endpoints from the network.
26	**Forensic Data Export**
	Must have an option to enable audit of Windows Authentication events, which allows Forensic Snapshots to contain more information on logon events.
27	**Remote Access**
	Must provide a command-line interface that can remotely access devices in order to perform a further investigation or take appropriate action.
28	**Endpoint + Email Gateway**
	Must be able to automatically isolate compromised mailboxes, and clean up infected computers sending outbound spam and malware.
29	**Endpoint + Firewall**
	Must be able to automatically isolate infected endpoints on the public and local area networks.
30	**Endpoint + Wireless Access Point**
	Must be able to restrict internet access for infected endpoints connected to Wi-Fi automatically.

Schedule -II

SPECIFICATIONS OF ANTIVIRUS SOFTWARE FOR SERVERS(ITEM @ S.NO 2)

	All End point Features with Manage Services for Servers
Sl No	***Added Services***
1	*Managed Service should provide 24/7 monitoring and Response*
2	*Managed Service should provide Proactive, manual response*
3	*Managed Service should provide Lead-driven threat hunting*
4	*Managed Service should provide Dedicated response lead*
5	*Machine-Accelerated Human Response*
6	*Complete Transparency and Control. (Notify, Collaborate & Authorize)*
7	*Direct Call-In Support*

Annexure - A

CHECKLIST (To be uploaded with Technical Bid)

S.no	Document to be uploaded in Technical bid on GEM	Whether Uploaded (Yes/No)
1.	Filled **Annexure - A**	
2.	Filled Details as per **Annexure-B** along with Complete tender document duly sealed and signed	
3.	Undertaking as per **Annexure – C on company Letter head**	
4.	Data Sheet(s) of the product offered in the bid are to be uploaded along with the bid documents. NAARM can match and verify the Data Sheet with the product specifications offered. In case of any unexplained mismatch of technical parameters, the bid is liable for rejection.	
5.	**Upload Manufacturer authorization: Wherever Authorized Distributors are submitting the bid, Manufacturers Authorization Form (MAF)/Certificate with OEM details such as name, designation, address, e-mail Id and Phone No. required to be furnished along with the bid.**	
6.	**Proof of Offered Product being listed in Gartner Leader/ Gartner Magic Qudrant.**	
7.	**Proof of Experience of 5 Years or more in Antivirus/Cyber Security sector. Supporting documents are to be provided along with filled Annexure - D**	
8.	**Certificate to the effect that Rates offered are those offered to Government/Academic institutions.**	
9.	**Provide Dedicated /Toll Free telephone number of Service & Support of your firm. BIDDER/OEM must have Dedicated/toll Free Telephone No. for Service Support.**	`
10	**Bidder/OEM must provide Escalation Matrix of Telephone Numbers for Service Support.**	
11	Scanned copy PAN & GSTIN Registration. (all scanned and combined in one pdf)	
12	The firm should enclose copies of income tax returns for the last 3 years (Financial Year 2017-18, 2018-19, 2019-20)	

Annexure - B

COMMERCIAL DETAILS

(To be submitted on Firm's Letter head)

1.	Name and Address of Bidder	
2.	Telephone No. / Mobile No. / FAX No.	
3.	Email ID	
4.	Month and Year of Establishment	
5.	PAN and GSTIN Number	

SIGNATURE OF THE BIDDER & STAMP

Date:

Place:

Annexure - C

UNDERTAKING

I/We have read and understood General Terms and Conditions contained in the ICAR-NAARM's Tender. I/We do hereby declare that all the details provided in this tender bid are true to the best of my/our knowledge and belief and any misrepresentation of facts will render me/us liable to any action as may be deemed fit by ICAR-NAARM, Hyderabad.

I/We do hereby also accept ICAR-NAARM have the right to accept or reject this application and not to issue invitation to Tender to me/us.

I/We undertake to communicate promptly to ICAR-NAARM any changes in the condition or working of the firm. It is also certified that we have not been blacklisted by any organization of Government of India including Central Vigilance commission (CVC) in the last three years. The undersigned is fully authorized to sign and submit this application form on behalf of the organization, he/she represent. We authorize ICAR-NAARM to approach individuals, employees, firms and corporations to verify our competence and general reputation.

I/We do hereby also certify that we have all the required experience in the relevant field for which bids are being invited by ICAR-NAARM.

AUTHORISED SIGNATORY OF THE FIRM WITH SEAL

Place:

Dated:

Annexure - D

RELEVANT WORK EXPERIENCE DETAILS

(To be submitted on Firm's Letter head)

Sr. No.	Name of the Deptt. Organization where work in Antivirus/Cyber Security sector was done	Period	
		From	To
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			

AUTHORISED SIGNATORY OF THE FIRM WITH SEAL

Place:

Dated: