वैज्ञानिक तथा औद्योगिक अनुसंधान परिषद्
Council of Scientific & Industrial Research
राष्ट्रीय वांतरिक्ष प्रयोगशालाएं
National Aerospace Laboratories

AS 9100:2016
Certified Organization

INVITATION FOR TENDERS

Tender No. NAL/PUR/ICTD/083/23 **Dated: 20/07/2023**

CSIR - National Aerospace Laboratories (NAL), Bengaluru, Karnataka, Republic of India, is one of the premier research laboratories under aegis of Council of Scientific and Industrial Research (CSIR), an autonomous body under the Department of Scientific and Industrial Research, Government of India, New Delhi. CSIR-NAL is a Science and Knowledge based Research, Development and Consulting Organisation. It is internationally known for its excellence in Scientific Research in Aerospace Engineering.

The Director, CSIR-NAL invites online quotation(s) for the procurement of the following item(s) for day to day research work.

Sl. No.	**Description of Item(s)**	**Unit**	**Quantity**
1	Unified Network Security Appliance with 3 years support (Please refer annexure for detailed specification)	No	01

Single / Double Bid Only	Single	Tender Type	Open
Bid Security (EMD) (in INR)	Bid Security Declaration should be enclosed with quotation	Bid submission end date	10-Aug-2023 10.00 Hrs
Performance Security	**3 per cent of the Purchase Order value**	Bid opening date	11-Aug-2023 11.00 Hrs

01. Tender document(s) may be downloaded from the Central Public Procurement Portal i.e., https://www.etenders.gov.in. Aspiring Bidders' who have not registered in the portal can do the same at free of cost before participating in our tendering process. Bidders are advised to go through instructions provided at 'Instructions for Online Bid Submission', in the portal.

02. Tenderer's can access tender document(s) on the website (for searching in the NIC site https://www.etenders.gov.in, kindly go to "Tender Search", option, select tender type and select 'Council of Scientific and Industrial Research', in organisation tab and select NAL-Bengaluru-CSIR in department type. Thereafter, Click on "Search", button to view all CSIR-NAL, Bengaluru tenders). Select the appropriate tender and fill them with all relevant information and submit the completed tender document online in the website as per the schedule given in the next page.

03. a. Global Tender Enquiry: Either the Indian Agent on behalf of the Foreign Principal or the Foreign Principal can bid directly in a tender but ***not*** both. However, the offer of the Indian Agent should also accompany the authorisation letter from their principal. To maintain sanctity of tendering system, one Indian Agent ***cannot*** represent ***two*** different Foreign Principals in ***one*** tender

b. Open Tender Enquiry: Only Local supplier's with prescribed local content as detailed in Department for Promotion of Industry and Internal Trade (DPIIT) Order No. P-45021/2/2017-PP (BE-II), dated 16th Sep, 2020, and subsequent orders issued by the Ministry of Finance, Government of India from time to time, are eligible for bidding. Bidders' must enclose the certificate declaring their local content of supplies as per our standard form.

Note: Kindly, refer to the first page of Notice Inviting Tender for tender type i.e. Open Tender Enquiry / Global Tender Enquiry and submit your bid accordingly.

04. Unsolicited / Conditional / Unsigned Quotations/Quotations received after the due date and time shall be summarily rejected. The Bidder should comply with the terms and conditions of the tender, failing which, their offer will be liable for rejection.

05. The bids' failing to comply with the following clauses will be summarily rejected.

a. The Bidders' proposing to supply finished products directly/indirectly from vendors' of countries sharing the land border with India should submit a copy of registration done with DPIIT.

b. If the products supplied are not from vendors of countries sharing land border with India, the Bidders' have to enclose a declaration to that effect.

06. As per Government of India procurement policies,

a. The purchaser intends to give purchase preference to local supplies (preference to Make in India) in case the cost of procurement is up to Rs. 50 (fifty) lakhs.

b. The procuring entity intends to give purchase preference to products/goods manufactured by Micro, Small and Medium Enterprises.

07. Bidders' are requested to refer to the instructions regarding Procurement Policies for "Make in India", issued by Ministry of Commerce and Industry, Department of Industrial Policy and Promotion dated. 28-May-2018, and 4-Jun-2020 and guidelines as and when issued.

08. Kindly, note CSIR-NAL **GST No. 29AAATC2716R1ZB.** And, the bidders' are requested to furnish their GST No. in their invoice failing which we will ***not*** be able to make timely payment.

09. Printed conditions, if any, submitted along with your quotation will not be binding on us.

10. The prospective bidders' are requested to refer to the Standard Terms and Conditions available on NAL Internet (www.nal.res.in) under the icon Tender-Purchase before formulating and submitting their bids'.

11. The Director, CSIR- National Aerospace Laboratories, Bengaluru, reserves the right to accept any or all the tenders either in part or in full or to split the order without assigning any reason(s) thereof.

Thanking you,

Yours faithfully

20/07/2023

Stores & Purchase Officer
For and on behalf of CSIR-NAL

TECHNICAL SPECIFICATIONS - UNIFIED NETWORK SECURITY APPLIANCE

Sl.No	Specification
1	Security solution must be appliance based without any user based licensing with AntiVirus, Web Filtering, QOS, Application Control & SSL + IPSEC VPN features inbuilt.
2	The proposed NGFW must protect from Known and unknown attacks using dynamic analysis and provide automated mitigation to stop attacks.
3	Security Solution should have inbuilt SD-WAN funtionality for supporting load balancing /express route selection based on SLA
4	The OEM quoted in bid must be Gartner's Leader in Network Firewall during 2019,2020,2021
5	The proposed Firewall should belong to a family of products that attains Recommended NSS Certification for NGFW during 2018 & 2019.
6	The OEM should have published all the performance mentioned on the corporate public website.
7	Security appliance should have a minimum throughput of 60 Gbps firewall throughput
	Security appliance should have a minimum storage of 480 GB
8	Should support at least 7 Million concurrent sessions & 500K new connections/sec
9	The firewall should do stateful inspection & must also support asymmetric routing if required
10	Should support Policy based routing, RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4
11	Multicasting must be supported in device
12	It should load balance & support automated Failover for 3 ISP's or more.
13	Security solution must support IP, MAC User based policies.
14	Security solution must integrate with Open LDAP, Radius, AD for user based policy.
15	Should support Active-Active & Active-standby when deployed in HA.
16	Should provide minimum Real world Threat Prevention Firewall throughput of 8 Gbps with Firewall, Application Control, anti-Malware enabled measured with (Real World / Enterprise Mix)
17	Solution should have WAN Path Controller and Link Health Monitoring for better application performance. Link Health monitor must identify latency, jitter and packet loss for each ISP.
18	Security solution must support Asset tagging to segregate secured, intellectual proprietary and unsecured devices. Based on the Asset should be able to define intent based policy.
19	Security solution should have comprehensive security controls on SSH Man-in-the-Middle(MITM) deep inspections. Like Inspection on tunnelled traffic and detect / prevent MITM attach etc..
20	Security solution must have the following support for IPv6 : Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, firewall for IPv6 traffic, NAT46, NAT64, IPv6 IPsec VPN
21	Security solution must support Active-passive, active-active and virtual clusters for high availability.
22	Security solution must have at minimum of 8 x1G SFP and 16 x 1GE RJ45 from day1.
23	Security solution must have at minimum of 8 x10G SFP+.Atleast 2 no's to be populated from day 1
24	Security solution must have dedicated console port RJ45 and 1 nos USB Port

20/07/2023

25	Security solution must have the capability to virtualize one physical firewall into minimum of 10 virtual firewalls.
26	Security solution must have minimum VPN throughput of 40 Gbps or more.
27	Security solution must support IPSec & 5000 SSL VPN. With necessary licenses from day1.
28	Should support the following IPSEC VPN deployment modes : Gateway-to-gateway, hub- and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,
29	Solution should have MAC host check per portal for SSL VPN
30	Security solution must support following OS (MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems) while connecting to office using SSL VPN.
31	Security solution must have Gateway Antivirus features in it which must support scanning for protocols such as SMTP/SMTPs, POP/POPs, HTTP/HTTPs.
32	It should be capable to detect & prevent virus such as Trojan, malwares, malicious data etc. at gateway level.
33	Security solution must offer anti-bot capabilities from day1. Add required licensing cost if it is an additional module.
34	Security solution must analyze BOT applications from client machines & must block all connections to C&C center.
35	Security solution should Detect unknown attacks using dynamic analysis and provides automated mitigation to stop targeted attacks .Cloud based Sandboxing License must be included.
36	Security solution should support be capable to remove exploitable content and replace it with content that is known to be safe. (CDR)
37	Security solution should have capability of virus outbreak Detection and prevention using checksums to filter files.
38	Security solution should Consist 200 Million URL's under 75+ Categories based web-sites filtering over ttp/https protocols by default excluding Custom URL / Category.
39	Security solution must understand websites of different languages & rate them.
40	It must support option to override the URL/category on User/User-group basis.
41	Security solution should support External Web Filter dynamic black lists which could be hosted on an HTTP server
42	Security solution should be able to block or allow matched Specific YouTube channels using Channel ID
43	Should be able to identify & control all commonly used web 2.0 applications & should be able to detect minimum 2500 applications.
44	It must support applications such as Torrent, P2P, Botnets, Games, Social networks irrespective of their websites.
45	Security solution should support to create custom application signatures.
46	Security solution should have capability to protect critical applications by enforcing granular application usage with traffic shaping.
47	Security Solution must have capability to identify the YouTube Video Name browsed by the end user.
48	Security solution should include Web Application Firewall feature with signatures for protecting from the attacks Cross Site Scripting, SQL Injection, Generic Attacks, Trojans, Information Disclosure, Known Exploits, Credit Card Detection, Bad Robot, etc
49	3 years of on-site comprehensive warranty, 24X7 support during the warranty, Warranty should cover the entire hardware and the software and include regular updates.

20/07/2023