National Rural Support Programme

Registered Office: UBL Building, 7th Floor, Jinnah Avenue, Blue Area, Islamabad.

Tel# 051-2822319

Programme Support Unit: IRM Complex, 7, Sunrise Avenue, Park Road, Chak Shehzad,

Near COMSATS University, Islamabad. Ph:051-8746170-3

Date: 19 July, 2026

RFP No. NRSP/FW/RQ-2634

Request for Proposals (RFP)

For the purchase of

NETWORK DETECTION AND RESPONSE

for

National Rural Support Programme (NRSP)

NRSP
National Rural Support Programme

REQUEST FOR PROPOSALS

National Rural Support Programme (NRSP) invites sealed proposals for the procurement of NETWORK DETECTION & RESPONSE from the registered suppliers/companies/ organizations/firms having past experience and valid NTN & GST, the details of equipment/services are given below: -

S.No	Description	Qty
1	NDR with all Allied accessories	01
2	Subscription & Support Licenses for 1 years	01
3	Deployment &Training for NRSP Staff	1 Job

Details and Terms & conditions are available in the documents that can be downloaded free of cost from NRSP web site **www.nrsp.org.pk/tenders/.** Last date for submission of sealed technical proposals is **4th August, 2026 till 3:00 pm** to the undersigned office at Islamabad. NRSP reserve the right to accept or reject any/all proposals without any reason thereof or funding constrains.

NRSP Administration, National Rural Support Programme,
IRM Complex, #7 Sunrise Avenue, Park Road, Chakshahzad,
Near COMSATS University, Islamabad,
Ph: 051-8746170-3
email: nrspprocurement@nrsp.org.pk

10x2

Details & Timelines of RFP		
1.	Date of availability of documents (RFP) on NRSP	**4th August 2026**
2.	Last date and time for sending queries/question or clarifications by suppliers	**24th July, 2026**
3.	Last date and time for reply of queries/question or clarifications by NRSP	**28th July 2026**
4.	Last date, time and address for receipt of Technical Proposals (in shape of hard copies)	**4th August, 2026 by 3:00 p.m.(PST)** NRSP Administration, National Rural Support Programme, #7 Sunrise avenue, Near COMSATS University, Park Road, Chak Shahzad, Islamabad, Tel:+92(51) 8746170-173
5.	Date and Time of Opening of Technical Proposals	**4th July, 2026 by 3:30 p.m.(PST)**
6.	Place of opening	National Rural Support Programme, #7 Sunrise avenue, Near COMSATS University, Park Road, Chak Shahzad, Islamabad, Tel:+92(51) 8746170-173
7.	Address for communication and correspondence	National Rural Support Programme, #7 Sunrise avenue, Near COMSATS University, Park Road, Chak Shahzad, Islamabad, Tel:+92(51) 8746170-173
8.	Contact for Firms	Interested Suppliers are requested to send their queries on the following email: nrspprocurement@nrsp.org.pk. The email query should clearly mentioned the following details, so that in case of any clarification, the same maybe issued to them: • Name of Company, Contact person, Mailing address, Telephone No. Email address, Mobile No. etc.

Note: Technical Proposals will be opened in presence of the supplier representative who choose to attend the opening session.

1. Introduction

Established in 1991, NRSP is the largest Rural Support Programme in the country in terms of outreach, staff and development activities. It is a not for profit organization registered under Section 42 of Companies Ordinance 1984.

NRSP's mandate is to alleviate poverty by harnessing people's potential and undertake development activities in Pakistan. It has a presence in 56 Districts in all the four Provinces including Azad Jammu and Kashmir through Regional Offices and Field Offices. NRSP is currently working with more than half a million poor households organized into a network of more than 115,076 Community Organizations. With sustained incremental growth, it is emerging as Pakistan's leading engine for poverty reduction and rural development.

2. Background

National Rural Support Programme (NRSP) is largest provider of Microfinance services in Pakistan. Since NRSP has deployed its IT system across NRSP branches network so there is need to implement NDR in NRSP data center. The detail specification of the required NDR is given below in section 3.

3. Procurement details.

The project scope spans around both data centers of NRSP Islamabad (Primary Site) and Lahore (DR) PTCL Garden Town. The selected firm will supply, install, configure, test, and support NDR and allied equipment. The selected firm will also be responsible for integrating the newly installed Solution with NRSP existing network completely end-to-end according to east/west and north/south traffic. The selected firm is expected to use the international 'best practices' in delivering the services with in time, cost and quality. Maintenance and support services will have to be provided by same firm during warranty period.

The successful firm will be responsible for:

a) Supply of proposed solution
b) Plan and Design
c) Complete Installation/Commissioning of proposed solution
d) Smooth and timely User Acceptance Test
e) Project management for supply of goods, support, warranty and services for the entire project.

Below is the complete list of NDR solution to be purchased under this tender.

Technical Specifications

NETWORK DETECTION & RESPONSE	
S#	**Technical Description, Specifications and Standards Required**
1	The proposed solution must be an on-premises hardware-appliance-based NDR platform
2	Should be capable of supporting minimum 1,000 IPs, or Higher
3	Should be scalable to large enterprise environments of up to 200K+ IPs under a single management and analytics framework, without performance degradation or re-architecture
4	A very high scalable platform that can support different options for Sensors and Analyzers/Brains, and to be fully analyzed by AI in a one rack unit analyzer with the different Sensors types (Virtual, Cloud, Physical) and sizes.
5	Have the option to deploy Log Collectors/sensors for the virtual environments (VMWare ESX, Hyper-V, KVM, Nutanix)
6	Have the option to deploy Cloud Sensors for IaaS (AWS, Azure, GCP)
7	Operate passive to the network i.e. not taxing network performance

8	Operate effectively and efficiently in a fully air-gapped environment, without requiring any persistent external connectivity, cloud dependency, or external telemetry.
9	Incorporate vendor-curated global attacker behavior models that can be manually and securely updated offline and deployed into air-gapped environments without transmitting NRSP data externally.
10	The solution must be agentless
11	Updates can be done Offline on the solution
12	The solution must not require traffic decryption
13	Ability to store the detections in the same Brain for 3-6 months along with its sample PCAP
14	Automatically identify and classify threats, including attack phase and risk, without requiring any manual work to build/tune the use cases
15	Must be on-prem and ability to work within air gapped environments
16	The proposed solution should be On Prem Appliance based.
17	The solution must rely primarily on behavioral and attacker-TTP-based detection, and must not depend on static signatures, simple heuristics, or IOC-only methodologies as its primary detection mechanism.
18	Differentiate key assets from other hosts for risk prioritization
19	Must have on single dashboard for detections that correlates Cloud/On-Prem/DC detections together automatically
20	Ability to automatically differentiate between general botnet behaviors and those that are more likely to be targeted threats
21	Ability to categorize the following Threats: • Botnet behavior including spam, DDoS, external vulnerability scanning, Bitcoin mining, etc. • Hidden tunnels within HTTP, HTTPS, and DNS used for command-and-control and data exfiltration. Without false positives due to standard beaconing from common tools and apps such as news tickers" will take out simple beacon detectors • The use of algorithmically generated domains or DGAs • Custom RATs (remote administration tools) from normal user traffic • Unknown command & control (no reputation history) using other traffic attributes • Data exfiltration independent of user identity or IP address • Internal reconnaissance of an attacker • Reconnaissance using slow or "paranoid" network scans • Improper use of administrative and management protocols, including RDP, SSH, iDRAC, and IPMI • Activation of sub-OS rootkits using port hijacking • Remote execution of procedure calls or code via SMB or DCERPC protocols • Privileged access analytics use cases by observing the privilege for the (account, host and service).
22	Solution must be protocol agnostic
23	Solution must provide an accounts-based view and prioritization based on threat and certainty scores
24	Using the AI to do the Triage and eliminate the manual work from the security teams and saving time and help the security teams to focus on what matters.
25	Automatically score and prioritize each individual attacker behavior detected
26	Automatically score and prioritize each host/account based on its behaviors over time (Focus on Attacker progress prioritization not just single event prioritization using AI)
27	Use the AI to do the prioritization based on attacker progression over the time.
28	Ability to notify staff based on the threat score
29	Provide elevated visibility of key assets with identified attacker behaviors
30	Provide individual scores for both threat and certainty / confidence
31	Provide visibility into host interconnectivity
32	Provide packet captures of identified attacker behaviors for analysis
33	Have the ability to find commonalities across multiple devices in the network and present it in a coherent attack campaign of all hosts participating in the campaign

34	Directly identify threats, based on network traffic analytics and depend on the behavioral models to find known and unknown without the need to decrypting the traffic. regardless of the signatures, IoC ...etc.
35	All detections capabilities must be fully onprem without any cloud components
36	Cover more than 90% of the MITRE ATT&CK network-based attackers Tactics
37	The platform must have patents that are referenced in MITRE D3FEND (Network Traffic Analytics)
38	Ability to detect attacker behaviors within encrypted traffic without decryption, using protocol semantics, traffic context, behavioral sequencing, and statistical indicators.
39	Detect custom or unknown threats, where there is no signature or IP/domain reputation history based on behavior
40	Solution to Focus on Attackers Behaviors (TTPs) not just simple anomaly models with generic ML approach.
41	Solution to be applicable across all user and infrastructure devices (Windows, Mac, mobile devices, byod, IoT, routers, TOR, firewalls)
42	Use a combination of deterministic behavioral models and machine-learning techniques (supervised, unsupervised, deep learning) to ensure detection accuracy, repeatability, and low false positives.
43	Solution must have the ability to analyze and correlate network traffic: North, South, East, West traffic
44	Solution must secure the data center within the virtual environment as well as the underlying infrastructure
45	Each detection must provide human-readable, explainable context, including why the behavior was flagged, which attacker techniques were observed, and how confidence and threat scores were calculated.
46	Automate threat hunting at wire speed
47	Ability to perform matching on IOCs introduced via STIX
48	The platform must be a privilege-aware platform (Host, account, and service privilege) that will learn it automatically and be used in Privileged Access Analytics. Using observed privilege to strengthen zero-trust access.
49	Solution must provide a clear quadrant style detection prioritization mapping Low, Medium, High and Critical hosts placed in the appropriate quadrant
50	Incorporate learnings from global attacker behaviors and techniques to detect threats on the local network whenever possible
51	Global modeling of threats to be combined with local network learning to improve accuracy and relevance for the local network
52	Detect potentially-malicious anomalies based on deviation from learned local norms within the network
53	Ability to detect threats within new devices or devices that were already compromised when baselined the solution must not use a generic approach to build it's unsupervised models
54	Maintain network packet captures of detected attacker behaviors and Must not decrypt the traffic in order to analyze
55	Solution must not use NetFlow/Logs as a data source and must use raw network traffic for real-time analysis
56	Provide limited time links of Hosts or Events for analysis by non-system users and Automate analysis to identify attacks
57	Ability to provide time-limited access to a specific event in the system with others without creating an account
58	All information about detections and hosts available via RESTful API to support automation
59	Detect the following type of threats (not limited to): - Remote access tunnels used by attackers to control compromised systems - Hidden tunnels over HTTP, HTTPS, or DNS to communicate with C&C or to exfiltrate data - Web-based Command and Control (not relying on IP reputation or threat lists) - Malware using a fake browser

	- Malware being updated - Multihomed domain fronting. - Relay hosts. - Malware getting new instructions - Malware replicating a payload to / exploiting vulnerabilities against other hosts - TOR Anonymization - Peer-to-peer traffic - Botnet monetization behaviors: Click Fraud, Bitcoin Mining, outbound DoS, outbound SPAM - Ransomware activity: encrypting file shares - Network reconnaissance scans: port scans, port sweeps, scanning unused IPs. - Privilege anomaly: to find use cases realter Privilege escalation, accounts take over, credentials theft and misuse. - Use of a stolen credential from a host it has not previously been used on - Use of a stolen credential from its normal system, but asking for unusual services or in excessive volume - A host trying many credentials to attempt to gain access to a server - Kerberos service scans - Fake Kerberos servers - Brute force attacks - RPC reconnaissance - Use of administrative protocols, including RDP, SSH, IDRAC, and IPMI, where the target host is not typically administered by the source host on that protocol - Activation of a sub-OS rootkit using an "knocking" byte sequence on a common port - A host gathering unusual volumes of data and then sending exfiltrating to an external IP - A host being used as a relay to exfiltrate data to an external system
60	Ability to detect enumeration of file shares
61	Ability to detect AD/LDAP reconnaissance using techniques similar to Bloodhound
62	Ability to detect use of PowerShell/WMI and RPC to move laterally via remote code execution
63	Ability to detect use of stolen RDP client tokens, RDP servers, RPC servers
64	Ability to detect the use of PS exec and other remote administration tools to move laterally via SMB
65	A host being used as a relay to exfiltrate data to an external system. A host being used as a relay for command and control purposes to gain access deeper into the network
66	Must natively integrate with some EDR Vendors, also have an API capable of integrating with others when needed. to support host lock down and enrich host dashboards
67	Solution must provide API-driven access to all events, hosts, and scoring information for integration with other security solutions (NAC, SOAR, FW, EDT) & operational systems
68	Account Lock down: Must natively integrate with AD: To allow immediate, customizable account enforcement via Active Directory integration. by surgically freeze account access and avoid service disruption by disabling accounts (auto and manual)
69	Must natively decapsulate the VxLAN/GRE traffic.
70	The solution must support automated updates where connectivity is permitted, and secure offline update packages for air-gapped environments, minimizing operational effort while maintaining full detection capability.
71	The solution must utilize Supervised Machine Learning models specifically trained on historical and real-world attacker behaviors (TTPs). The system must be capable of distinguishing between 'benign anomalies' (e.g., a software update or new admin activity) and 'malicious signals' (e.g., lateral movement or reconnaissance), ensuring that high-severity alerts are prioritized based on attack intent rather than simple statistical deviation
72	The platform must extract and store enriched network metadata (not just NetFlow or PCAP) for a minimum of 30 days locally/on-cloud. This metadata must be indexed and searchable in real-time, allowing security analysts to perform retroactive 'Threat Hunting' queries across 40+ network protocols (including Kerberos, RPC, and DNS) without the need to replay raw packets.

73	When suspicious activity is identified and alerted upon it is critical that the system provide appropriate commentary around the detection including appropriate triggers as well as steps to verify and where to begin potential remediation
74	The solution must enrich its metadata/detections/hosts with the info that will help improve the IR approach, natively and without complex integrations (Host IID)
75	The solution must provide unified entity attribution that correlates network metadata with identity-based signals (Active Directory/Azure AD) to maintain a persistent 'Threat & Certainty' score for a single user/host, even as they move across different IP addresses, VLANs, or hybrid-cloud environments
76	In order for a fully effective deployment the solution must not requiring any third-party object configuration changes (except for span/tap/mirror) such as adding additional locations for logging destinations.
77	The solution must feature dedicated, non-signature-based AI models specifically trained to detect 'Hidden Command & Control (C2)' and 'Data Exfiltration' via HTTPS/DNS tunnels, with the ability to map these detections directly to specific MITRE ATT&CK techniques without requiring manual rule tuning
78	The platform must utilize an automated prioritization engine that plots detections on a 2D quadrant of 'Threat Severity' vs. 'Certainty of Attack.' The solution must automatically surface only high-fidelity 'Critical' and 'High' quadrants for immediate SOC action, rather than a chronological list of all detected anomalies
79	The proposed Network Detection and Response (NDR) solution must be capable of passively ingesting network traffic for analysis. This data ingestion shall be achieved by connecting to a network switch's Switch Port Analyzer (SPAN) or a network Test Access Port (TAP) at key points within the network infrastructure.
80	Must be able to provide health monitoring via email and syslog.
81	Must be able to alert on individual threats or suspicious hosts via email and syslog
82	Must provide granular role-based access control (RBAC) into the various elements of the product so security analysts can define custom roles with limited access if desired
83	Must have the ability to send audit log over syslog for actions such as login, logout and changes to settings that impact the security posture of the product
84	The technology vendor should be NDR focused and must have at least 35 technology patents or higher
85	The vendor must provide independent third-party validation (e.g., Gartner, MITRE ATT&CK Evaluations, peer-reviewed research, or equivalent) that supports the effectiveness of behavior-based detection of attacker techniques, not merely anomaly detection or reputation-based approaches.

4. Requirements

a) Installation and configurations with respect to NRSP Network design and NRSP Business requirements at PR site.
b) The successful supplier must provide planning & design document by following industry best practices.
c) The successful supplier is expected to integrate new work seamlessly into the existing network infrastructure, understand existing setup and implement all changes as per business need.
d) Supplier must execute necessary configuration changes to newly & existing all devices to support the newly contracted work, where required to complete the assignment.
e) The supplier should provide a plan for support, warranty and services in its technical proposal.
f) Each and every part/ component required to operate hardware being procured or license(s), should be included in deliverable (technical and financial Proposal) and shall be the responsibility of the supplier.
g) Undertaking for not blacklisted as per provided format.
h) Only brand-new hardware to be proposed. Refurbished, Grey or smuggled or international warranty products will be not accepted in any case.

5. Eligibility of the Supplier

Following is the eligibility criteria to participate (Refer to Form E1)

a) Must be registered with SECP or Registrar of Firms in Pakistan and working for the last 5 years in Pakistan in the field of IT (Certificate of Incorporation to be attached from SECP or Registrar of Firms)
b) Must have valid/active NTN and GST and on active tax payer list of FBR on the date of submission of proposal
c) Must be authorized partner of the proposed solution and must provide Manufacturer Authorization Letter (MAL) with reference to this tender to participate in this tender
d) Must have at least 3 years of experience in selling proposed type of solution. (Attach at least three documentary evidences in shape of completion certificates / POs)
e) Must have at least two certified professionals from OEM locally (Islamabad & Lahore) of proposed type of solution to support the offered equipment. (Current CVs with valid certification from OEM to be attach with the technical proposal)
f) Proposed Solution must be listed in Latest Gartner Magic (Leaders) Quadrant for Network Detection & Response (evidence to be attached with the technical proposal)
g) Must have Minimum 2 Deployments by OEM including banking/financial/Public/Private sectors in Pakistan (Share the complete list with contact person details for verification purpose with the technical proposal)
h) Must natively integrate with SIEMs (LogRhythm) (Attach Compatibility list)
i) Must quote onsite Installation and Trainings by OEM
j) Must Quote (one) Year 24/7/365 Technical OEM & Supplier support (parts and services both) from the date of commissioning
k) Undertaking of blacklisting as per Form E1.1

6. Submission of Proposals

Proposals will be accepted and evaluated using **Two Stage – Single Envelop Procedure**, The Technical and Financial proposals shall be submitted in a separate sealed envelope clearly mentioned. At first stage only technical proposal should be opened. Technical and Financial Proposals marked as: -

Technical Proposal - RFP No. NRSP/FW/RQ-2634

&

Financial Proposal – RFP No. NRSP/FW/RQ-2634

The cover letter should also specify the validity date of each proposal with point of contact (name, email & contact cell number) for this RFP from supplier side.

I. The **technical proposal** shall provide/contain the following information/documents:

i. Technical Proposal Submission Form (Form T1)
ii. Mandatory Eligibility Criteria (Form E1)
iii. Technical Compliance sheet
iv. Company Profile and Copy of last financial year audit report dully signed by the auditor
v. Specific experience for similar assignments.
vi. General experience.
vii. Qualification and Competence of the proposed team for support for this assignment.
viii. Proposed solution compliance with required specifications, delivery time, installation/ testing/ commissioning plan.

ix. Proposed solution with make and model, SLA details, Subscription & Support details and training details. All the relevant literature, catalogs, broachers must be attached showing the technical specifications in details with technical compliance sheet.

x. Any other document which could be helpful in the technical evaluation.

xi. Project Implementation Plan

The technical proposal shall not include any financial information.

II. The **financial proposal** shall contain the following information:

i. Financial Proposal Submission Form (Form F1)

ii. The DDP (Ex-Islamabad NRSP Data Center & Ex- Lahore NRPS DR Site) price of each item with complete details, make and model. All applicable taxes and mentioned clearly. Prices should be on DDP. (Form F2)

iii. Delivery time required for each item. (Form F2)

iv. Supply, installation, testing and configuration details. (Form F2)

v. Bid Security @2% of the total deliverable (including taxes) in the shape of Call deposit/Pay Order/Demand Draft/cashier cheque in the name of NRSP.

vi. Validity of the financial proposal. (Form F2)

vii. Other terms and conditions (if any).

a) Suppliers must offer complete solution with training as given in section 3. Incomplete or partial proposals will be rejected.

b) If the proposal is not submitted in the prescribed formats or any of the item in the as mentioned above, the proposal may be rejected. All the required documents must be attached/provided.

c) Once the proposal is submitted in sealed cover by the supplier, NRSP will not accept any addition / alterations / deletions of the proposal. However, NRSP reserves the right to seek clarification or call for supporting documents from any/all of the suppliers, for which the concerned supplier will need to submit the documentary evidence(s) as required by NRSP.

d) Any Proposal, submitted with incorrect information will be liable for rejection. Further, if any supplier is found to have submitted incorrect information at any time, his proposal will be rejected and he may be debarred from participation in the future tendering processes.

e) The Supplier should take care in submitting the proposals and ensure that enclosed papers are not found loose and should be **properly numbered** and submitted in a file in proper manner so that the papers do not bulge out and tear during scrutiny.

f) **Last Date of Submission is 4th August, 2026 till 3:00 pm local time. Supplier should be responsible to submit the proposal on time. Any delay from courier or rider will be on NRSP account. NRSP will close the Proposals receiving on above given date and time.**

g) The proposals must be submitted in original hard copy not later than **4th August, 2026 till 3:00 pm** local time to the point of contact given below. Electronic proposals will not be entertained. Any proposals delivered after due date and time will be considered as non-responsive and disqualified from further consideration.

h) The proposals should be marked/addressed as:

(Proposal for NETWORK DETECTION & RESPONSE Solution for NRSP)
RFP No. NRSP/FW/RQ-2634
NRSP Administration,
National Rural Support Programme
IRM Complex, 7, Sunrise Avenue, Park Road, Chak Shehzad,
Near COMSATS University, Islamabad.
Ph:+92-51-8746170-3.

i) NRSP reserves the right for conducting pre-shipment inspection by its own personnel or reputed third parties. The selected supplier has to offer the solution for inspection in such a manner that it does not affect the delivery schedule.

j) The offer should remain valid for a period of **90 days** from the closing/submission date. Any offer falling short of the validity period is liable for rejection. If a supplier extend proposal validity period, then will also extend the security period.

k) Alternative option, if there is any alternate option then it mentioned separately in proposal. Alternative options benefits should be clearly mentioned.

l) Clearance of the equipment from Tax Authorities would be the responsibility of the supplier.

m) Selected supplier must undertake to provide NRSP, the consignment notes number(s) by which the equipment ordered had been dispatched from their site, so as to have online / web access to the tracking system of physical movement of the consignments sent through courier.

n) The supplier may withdraw its offer after its submission, provided that written notice of withdrawal is received by NRSP prior to the closing date and time prescribed for submission of proposals. No offer can be withdrawn by the supplier subsequent to the closing date and time for submission of proposals.

7. Evaluation Criteria

Supplier has to fulfill the eligibility criteria initially. After qualifying the eligibility criteria, technically evaluation will be checked as per compliance sheet provided in this document. After technical compliance and evaluation, successful suppliers will be called to submit financial proposals. Financial proposals will be opened in front of all suppliers. Financial lowest proposal, fulfilling all criteria (eligibility and technical), will be shortlisted for award.

NRSP will scrutinize the proposals to determine whether it is complete, whether errors have been made in the offer, whether required technical documentation has been furnished and whether the documents have been properly signed. Offers with incorrect information or not supported by documentary evidence, wherever called for, would be summarily rejected. However, NRSP, at its sole discretion, may waive any minor non -conformity or any minor irregularity in an offer. NRSP reserves the right for such waivers and this shall be binding on all suppliers.

For proper scrutiny, evaluation and comparison of offers, NRSP, at its discretion, may ask some or all suppliers for clarification of their offer. The request for such clarifications and the response will necessarily be in writing.

8. Deliverables

Solution and software as per details given section 3.

9. Terms of Proposal

a) Bid Security

All suppliers shall furnish bid security deposit equivalent to **2% of the total Cost of Deliverables** (including taxes) in the form of Call deposit/Pay Order/Demand Draft in favor of NRSP. Cheque will not be accepted in any case. After selection of successful supplier, NRSP will return/release the bid security to the unsuccessful suppliers. NRSP NTN number is 0656952-8.

b) Performance Security

Performance security will be 5% of the total cost of the solution (excluding training) which will be withheld from the final payment for the period of three years. After the successful completion of warranty period of three years, performance security will be released. The amount withheld may be released against the bank guarantee from a schedule bank of same amount provided by the supplier as performance guarantee.

10. Fees and payment Schedule

a) Payment will be made after the complete and satisfactory delivery/acceptance of solution within 2-3 weeks through cross cheque in favour of supplier or as agreed at the time of contract.

b) Taxes will be deducted from all the invoices as per prescribed law of Govt. of Pakistan. If supplier has any of the tax exemption, the details must be attached with the invoice. Tax challans will be provided within 3-4 weeks of the payment.

11. Paying Authority

The payments as per the Payment Schedule covered hereinabove shall be paid by NRSP. However, Payment of the bills would be payable on receipt of advice/confirmation for satisfactory delivery / installation / configuration from Network Administrator and Programme Manager IT.

Following Documents are to be submitted for Payment:

a. Bill
b. GST Invoice
c. Duly acknowledged Delivery Challan/acceptance Certificate.

12. Delivery Schedule

a) The Selected supplier must undertake to deliver the equipment ordered 10-12 Weeks, to NRSP Data Center Sihala Islamabad and DR site Lahore within the time offered in the proposals from the date of the Purchase Order/Contact. However, Delivery schedule may be changed under special circumstances at the discretion of NRSP.

b) NRSP reserves right to shift the ordered equipment to any location where it has presence, anywhere in Pakistan, either during the warranty.

13. Warranty & Maintenance

The supplier shall be fully responsible for the defected items and will be responsible to replace at his own cost with the same make/model of the solution. All the proposed solution should have three years warranty (24/7/365) from the date of commissioning as mentioned in the section 3.

14. Penalty for Downtime

In case of delay in the supply of material against the terms indicated in the purchase order/contract, the supplier will have to pay a fine of 0.5 % (Half) percent of the balance qty for each day of delay. Maximum penalty will be 10% of the total order/contract. If shipment is delayed for more than 20 days NRSP has the right to unilaterally cancel the PO/contract and supplier bid security will be forfeited.

15. Penalty on Liquidated Damages for delayed supply

In case the delivery is delayed beyond the stipulated date of delivery, 'Liquidated damage for late delivery @ one half of one percent (0.5%) of the order value for each day of delay or part thereof would be imposed, subject to maximum of 10% if the delay is for 20 days or more. The penalty for late delivery will be deducted from the final invoice amount.

16. Currency

All prices shall be expressed in Pakistani Rupees only.

17. Cost of Process

The supplier shall bear all the costs associated with the preparation and submission of proposals & samples (if any) and NRSP will in no case be responsible or liable for these costs regardless of the conduct or outcome of the procurement process.

18. Tender Document

The supplier is expected to examine all instructions, forms, Terms and Conditions and specifications in the Tender Document. Submission of a proposal not responsive to the Tender Document in every respect will be at the supplier's risk and may result in the rejection of its proposal without any further reference to the supplier.

19. Deadline for Submission of proposals

Proposals must be received by NRSP at the address specified in the Tender Document not later than the specified date and time as specified in the Tender Document. In the event of the specified date of submission of proposals being declared a holiday for NRSP, the proposals will be received up to the appointed time on next working day.

NRSP may, at its discretion, extend this deadline for submission of proposals by amending the Tender documents.

20. Confidentiality Statement

All data and information received from NRSP for the purpose of this assignment is to be treated confidentially and is to be used ONLY in connection with the execution of these documents. All intellectual property rights arising from the execution of these documents are assigned to NRSP. The contents of written materials obtained and used in this assignment may not be disclosed to any third parties without the expressed advance written authorization of NRSP.

NRSP may then disclose the draft, final report and/or any related information to any person and for any purpose they may deem appropriate.

21. General Terms & Conditions

NRSP does not bind itself to accept the lowest or any proposal and reserves the right to reject any or all proposals at any point of time prior to the issuance of purchase order/contract without assigning any reasons whatsoever.

a. The NRSP reserves the right to resort to re-tendering without providing any reason whatsoever. The NRSP shall not incur any liability on account of such rejection.
b. The NRSP reserves the right to modify any terms, conditions or specifications for submission of offer and to obtain revised proposals from the suppliers due to such changes, if any.
c. Canvassing of any kind will be a disqualification and the NRSP may decide to cancel the supplier from its empanelment.
d. Supplier code of conduct is attached for required compliance as Annex A.

22. Rejection of the Proposal

The proposal is liable to be **rejected** if:

a. The document doesn't bear signature of authorized person.
b. It is received through E-mail or whatsapp.
c. If the proposal is submitted without or less or not in required type the bid security deposit.
d. If the technical proposal is submitted without the Technical Compliance Sheet.
e. If the proposal is received after expiry of the due date and time stipulated for proposal submission, due to any reason.
f. If the proposal is for refurbished, grey or smuggled or international warranty products.
g. If the financial proposal is submitted with the technical proposal or technical proposal contains any financial information
h. Incomplete proposals, partial proposals including non-submission or non-furnishing of requisite documents / Conditional proposals / proposals not conforming to the terms and conditions stipulated in this tender document are liable for rejection by the NRSP.

23. Modifications and Withdrawal of Proposals

Proposals once submitted will be treated, as final and no further correspondence will be entertained on this.

a. No proposal will be modified after the deadline for submission of proposals.

b. No supplier shall be allowed to withdraw the proposal, once the first technical proposal is opened.
c. No supplier shall be allowed to withdraw the proposal, if the supplier happens to be a successful supplier.

24. Proposal Opening and Evaluation

a. NRSP will open the proposals, in the presence of supplier's representative(s) who choose/authorized to attend, at the time and date mentioned in document at the address mentioned.
b. The supplier's representatives who are present shall sign the sheet evidencing their attendance. In the event of the specified date of proposal opening being declared a holiday for Purchaser, the proposals shall be opened at the appointed time and place on next working days.
c. Suppliers fulfilling the eligibility criteria, satisfying the technical requirements as determined by NRSP Technical Team and accepting the Terms and Conditions of this document shall be short-listed.
d. Decision of NRSP in this regard shall be final and binding on the suppliers.
e. The contract will be awarded only to the successful responsive supplier.
f. NRSP reserves the right to negotiate with second and third supplier etc. if successful supplier is not able to supply the deliverables and his bid security will be forfeited.

25. Clarifications of Proposals

To assist in the examination, evaluation and comparison of proposals NRSP may, at its discretion, ask the supplier for clarification. The response shall be in writing and no change in the substance or price of the proposal shall be sought, offered or permitted.

26. NRSP's Right to Accept or Reject Any Proposal Or All proposals

NRSP reserves the right to accept or reject any proposal and annul the procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected supplier or suppliers or any obligation to inform the affected supplier or suppliers of the ground for NRSP's action.

27. Governing Laws and Disputes

All disputes or differences whatsoever arising between the parties out of or in relation to the meaning and operation or effect of these Tender Documents or breach thereof shall be settled amicably. If however the parties are not able to solve them amicably, the same shall be settled by arbitration in accordance with the applicable Pakistani Laws, and the award made in pursuance thereof shall be binding on the parties. The Arbitrator/Arbitrators shall give a reasoned award.

28. Placement of Order and Acceptance

The supplier shall give acceptance of the order placed within 7 days from the date of order, failing which, NRSP shall have right to cancel the order.

29. Authorized Signatory

The supplier should indicate the authorized officials from their organization who can discuss, correspond, sign agreements / contracts, raise invoice and accept payments and also to correspond. The suppliers should furnish proof of signature of the authorized personnel for above purposes *as* required by the NRSP.

30. Appeals

Suppliers believing that they have been harmed by an error or irregularity during the evaluation or award process may file a complaint to NRSP only at complaints@nrsp.org.pk. No complaint will be entertained if filed by any other mean/platform.

STANDARD FORMS

Form E1

	MANDATORY ELIGIBILITY CRITERIA	**Yes**	**No**
1	Must be registered with SECP or Registrar of Firms in Pakistan and working for the last 5 years in Pakistan in the field of IT (Certificate of Incorporation to be attached from SECP or Registrar of Firms with the technical proposal).	☐	☐
2	Must have valid/active NTN and GST and on active tax payer list of FBR (copy of NTN and GST certificate to be attached with the technical proposal)	☐	☐
3	Supplier must be authorized partner of the proposed solution and must provide Manufacturer Authorization Letter (MAL) to participate in this tender.(to be attached with the technical proposal)	☐	☐
4	Must have at least 3 years of experience in selling proposed type of solution. (Attach at least three documentary evidences in shape of completion certificates / POs to be with the technical proposal)	☐	☐
5	Must have at least two certified professionals from OEM locally (Islamabad and Lahore) of proposed solution to support the offered equipment.(Current CVs with valid certification from OEM to be attached with the technical proposal)	☐	☐
6	Proposed Solution must be listed in Latest Gartner Magic (Leaders) Quadrant for Network Detection & Response (Report Attached with the technical proposal)	☐	☐
7	Must have Minimum 2 Deployments by OEM including banking/financial/Public/Private sectors in Pakistan (Share the complete list with contact person details for verification purpose with the technical proposal)	☐	☐
8	Must natively integrate with some SIEM/Datalake Vendors (Attach Compatibility list)		
9	Must quote Onsite Installation and Trainings by OEM	☐	☐
10	Must Quote 1 Years 24/7/365 Technical OEM & Supplier support (parts and services both) from the date of commissioning	☐	☐
11	Affidavit (on Rs.100/- stamp paper) dully signed and attested by Notary public as per format provided in From E1.1 with the technical proposal	☐	☐

Signature: _____

Name: _____

Date: _____

Form E1.1

DECLARATION OF ELIGIBILITY

(SHOLD BE SUBMITTED ON RS.100- STAMP PAPER DULLY ATTESTED BY NOTARY PUBLIC)

In the response to your RFP No. NRSP/FW/RQ-2634, I/We, the undersigned, hereby declare that:

- Our proposal/bid is valid for a period of 90 days from the last date for the submission.
- We agree to adhere to all of the terms and conditions as given in the tender documents of the NRSP and other documents as provided in the tender documents.
- We confirm that we are not engaged in any corrupt, fraudulent, collusive or coercive practices and acknowledge that if evidence contrary to this exists, NRSP reserves the right to reject our proposal/bid or terminate the contract with immediate effect.
- We are not bankrupt or being wound up, are having our affairs administered by the courts, have not the subject of proceedings concerning those matters, or are in any analogous arising from the, a procedure provided for in national legislation or regulations.
- We have not been convicted of an offence concerning professional conduct by any judgment.
- We have not been guilty of grave professional misconduct proven by any means which the NRSP can justify.
- We have fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with legal provision the country in which we are established or with those of the country where the contract is to be performed.
- Have no relation, direct or indirect, with proscribed individual/entities/political exposed person/s or terrorists organizations.
- Not or never prosecuted under Schedule 4 of the proscribed persons under NACTA for AML/CFT.
- We have not been the subject of the judgment for any fraud, corruption, involvement in criminal/terrorist organization or any other illegal activity detrimental to Pakistani Law.
- I/We as sole proprietorship, authorized dealers, Association of Persons (AOP), partnership firms, private or public limited companies or other do not have any kind of relationship with the NRSP Staff; and if later my this statement is not found in conformity with reality i.e. relationship is found, I would stand liable to NRSP as per the rules mentioned in the tender documents.
- Are not guilty of serious misinterpretation in supplying information.
- Are not in situations of conflict of interest (with prior relationship to project or family or business relationship to parties in NRSP).
- Have no relation, direct or indirect, with any terrorist or banned organizations.
- Are not blacklisted by any Local/International organization, PPAR, SPPRA, Government/semi Government department, NGO or any other company/organization.
- Have no relation, direct or indirect, with proscribed individual/entities/political expose person(s).
- Are not on any list of sanctioned parties issued by the Pakistan Government, DIFD, USAID, UN agencies, UNSCR, NACTA, European Union and others.
- Have not been reported for/under litigation for child abuse.

Full official Name: _____
CNIC No: _____
Name of Company: _____
Signature: _____
Company Stamp: _____

(Should be attested by Notary Public)

Form T1

TECHNICAL PROPOSAL SUBMISSION FORM

[*Date*]

To:

Procurement Committee,
National Rural Support Programme,
IRM Complex, 7th Sunrise Avenue, Park Road,
Near COMSATS University, Islamabad.
Tel: (92-51) 8746170-73

Subject: Submission of Technical proposal RFP No. NRSP/FW/RQ-2634

Sir,

We, the undersigned, offer to provide the equipment & services for NRSP, in accordance with your Request for Proposal dated 4th August 2026. We are hereby submitting our Technical Proposal.

Our Proposal is binding upon us and subject to the modifications resulting from Contract negotiations. We understand that NRSP may accept or reject our proposal without giving any reason.

We understand you are not bound to accept any Proposal you receive.
We remain,

Yours sincerely,

Authorized Signature:
Name and Title of Signatory:
Name of Firm:
Address:
Email:
Contact No.:

Technical Compliance Sheet for Solution

NETWORK DETECTION & RESPONSE

S#	Technical Description, Specifications and Standards Required	Compliance Yes / No
1	The proposed solution must be an on-premises hardware-appliance-based NDR platform	
2	Should be capable of supporting minimum 1,000 IPs, or Higher	
3	Should be scalable to large enterprise environments of up to 200K+ IPs under a single management and analytics framework, without performance degradation or re-architecture	
4	A very high scalable platform that can support different options for Sensors and Analyszers/Brains, and to be fully analyzed by AI in a one rack unit analyzer with the different Sensors types (Virtual, Cloud, Physical) and sizes.	
5	Have the option to deploy Log Collectors/vSensors for the virtual environments (VMWare ESX, HyperV, KVM, Nutanix)	
6	Have the option to deploy Cloud Sensors for IaaS (AWS, Azure, GCP)	
7	Operate passive to the network i.e. not taxing network performance	
8	Operate effectively and efficiently in a fully air-gapped environment, without requiring any persistent external connectivity, cloud dependency, or external telemetry.	
9	Incorporate vendor-curated global attacker behavior models that can be manually and securely updated offline and deployed into air-gapped environments without transmitting NRSP data externally.	
10	The solution must be agentless	
11	Updates can be done Offline on the solution	
12	The solution must not require traffic decryption	
13	Ability to store the detections in the same Brain for 3-6 months along with it's sample PCAP	
14	Automatically identify and classify threats, including attack phase and risk, without requiring any manual work to build/tune the use cases	
15	Must be on-prem and ability to work within airgapped environments	
16	The proposed solution should be On Prem Appliance based.	
17	The solution must rely primarily on behavioral and attacker-TTP-based detection, and must not depend on static signatures, simple heuristics, or IOC-only methodologies as its primary detection mechanism.	
18	Differentiate key assets from other hosts for risk prioritization	
19	Must have on single dashboard for detections that correlates Cloud/On-Prem/DC detections together automatically	
20	Ability to automatically differentiate between general botnet behaviors and those that are more likely to be targeted threats	
21	Ability to categorize the following Threats: • Botnet behavior including spam, DDoS, external vulnerability scanning, Bitcoin mining, etc. • Hidden tunnels within HTTP, HTTPS, and DNS used for command-and-control and data exfiltration. Without false positives due to standard beaconing from common tools and apps such as news tickers" will take out simple beacon detectors • The use of algorithmically generated domains or DGAs • Custom RATs (remote administration tools) from normal user traffic • Unknown command & control (no reputation history) using other traffic attributes • Data exfiltration independent of user identity or IP address • Internal reconnaissance of an attacker • Reconnaissance using slow or "paranoid" network scans	

	• Improper use of administrative and management protocols, including RDP, SSH, iDRAC, and IPMI • Activation of sub-OS rootkits using port hijacking • Remote execution of procedure calls or code via SMB or DCERPC protocols • Privileged access analytics use cases by observing the privilege for the (account, host and service).	
22	Solution must be protocol agnostic	
23	Solution must provide an accounts based view and prioritization based on threat and certainty scores	
24	Using the AI to do the Triage and eliminate the manual work from the security teams and saving time and help the security teams to focus on what matters.	
25	Automatically score and prioritize each individual attacker behavior detected	
26	Automatically score and prioritize each host/account based on its behaviors over time (Focus on Attacker progress prioritization not just single event prioritization using AI)	
27	Use the AI to do the prioritization based on attacker progression over the time.	
28	Ability to notify staff based on the threat score	
29	Provide elevated visibility of key assets with identified attacker behaviors	
30	Provide individual scores for both threat and certainty / confidence	
31	Provide visibility into host interconnectivity	
32	Provide packet captures of identified attacker behaviors for analysis	
33	Have the ability to find commonalities across multiple devices in the network and present it in a coherent attack campaign of all hosts participating in the campaign	
34	Directly identify threats, based on network traffic analytics and depend on the behavioral models to find known and unknown without the need to decrypting the traffic. regardless of the signatures, IoC ...etc.	
35	All detections capabilities must be fully onprem without any cloud components	
36	Cover more than 90% of the MITRE ATT&CK network based attackers Tactics	
37	The platform must have patents that are referenced in MITRE D3FEND (Network Traffic Analytics)	
38	Ability to detect attacker behaviors within encrypted traffic without decryption, using protocol semantics, traffic context, behavioral sequencing, and statistical indicators.	
39	Detect custom or unknown threats, where there is no signature or IP/domain reputation history based on behavior	
40	Solution to Focus on Attackers Behaviors (TTPs) not just simple anomaly models with generic ML approach.	
41	Solution to be applicable across all user and infrastructure devices (Windows, Mac, mobile devices, byod, IoT, routers, TOR, firewalls)	
42	Use a combination of deterministic behavioral models and machine-learning techniques (supervised, unsupervised, deep learning) to ensure detection accuracy, repeatability, and low false positives.	
43	Solution must have the ability to analyze and correlate network traffic: North, South, East, West traffic	
44	Solution must secure the data center within the virtual environment as well as the underlying infrastructure	
45	Each detection must provide human-readable, explainable context, including why the behavior was flagged, which attacker techniques were observed, and how confidence and threat scores were calculated.	
46	Automate threat hunting at wire speed	
47	Ability to perform matching on IOCs introduced via STIX	

48	The platform must be a privilege-aware platform (Host, account, and service privilege) that will learn it automatically and be used in Privileged Access Analytics. Using observed privilege to strengthen zero-trust access.	
49	Solution must provide a clear quadrant style detection prioritization mapping Low, Medium, High and Critical hosts placed in the appropriate quadrant	
50	Incorporate learnings from global attacker behaviors and techniques to detect threats on the local network whenever possible	
51	Global modeling of threats to be combined with local network learning to improve accuracy and relevance for the local network	
52	Detect potentially-malicious anomalies based on deviation from learned local norms within the network	
53	Ability to detect threats within new devices or devices that were already compromised when baselined the solution must not use a generic approach to build it's unsupervised models	
54	Maintain network packet captures of detected attacker behaviors and Must not decrypt the traffic in order to analyze	
55	Solution must not use NetFlow/Logs as a data source and must use raw network traffic for real-time analysis	
56	Provide limited time links of Hosts or Events for analysis by non-system users and Automate analysis to identify attacks	
57	Ability to provide time-limited access to a specific event in the system with others without creating an account	
58	All information about detections and hosts available via RESTful API to support automation	
59	Detect the following type of threats(not limited to): - Remote access tunnels used by attackers to control compromised systems - Hidden tunnels over HTTP, HTTPS, or DNS to communicate with C&C or to exfiltrate data - Web-based Command and Control (not relying on IP reputation or threat lists) - Malware using a fake browser - Malware being updated - Multihomed domain fronting. - Relay hosts. - Malware getting new instructions - Malware replicating a payload to / exploiting vulnerabilities against other hosts - TOR Anonymization - Peer-to-peer traffic - Botnet monetization behaviors: Click Fraud, Bitcoin Mining, outbound DoS, outbound SPAM - Ransomware activity: encrypting file shares - Network reconnaissance scans: port scans, port sweeps, scanning unused IPs. - Privilege anomaly: to find use cases realter Privilege escalation, accounts take over, credentials theft and misuse.- Use of a stolen credential from a host it has not previously been used on - Use of a stolen credential from its normal system, but asking for unusual services or in excessive volume - A host trying many credentials to attempt to gain access to a server - Kerberos service scans - Fake Kerberos servers - Brute force attacks - RPC reconnaissance - Use of administrative protocols, including RDP, SSH, IDRAC, and IPMI, where the target host is not typically administered by the source host on that protocol - Activation of a sub-OS rootkit using an "knocking" byte sequence on a common port - A host gathering unusual volumes of data and then sending exfiltrating to an external IP - A host being used as a relay to exfiltrate data to an external system	
60	Ability to detect enumeration of file shares	

61	Ability to detect AD/LDAP reconnaissance using techniques similar to Bloodhound	
62	Ability to detect use of PowerShell/WMI and RPC to move laterally via remote code execution	
63	Ability to detect use of stolen RDP client tokens, RDP servers, RPC servers	
64	Ability to detect the use of PS exec and other remote administration tools to move laterally via SMB	
65	A host being used as a relay to exfiltrate data to an external system. A host being used as a relay for command and control purposes to gain access deeper into the network	
66	Must natively integrate with some EDR Vendors, also have an API capable of integrating with others when needed. to support host lock down and enrich host dashboards	
67	Solution must provide API-driven access to all events, hosts, and scoring information for integration with other security solutions (NAC, SOAR, FW, EDT) & operational systems	
68	Account Lock down: Must natively integrate with AD: To allow immediate, customizable account enforcement via Active Directory integration. by surgically freeze account access and avoid service disruption by disabling accounts (auto and manual)	
69	Must natively decapsulate the VxLAN/GRE traffic.	
70	The solution must support automated updates where connectivity is permitted, and secure offline update packages for air-gapped environments, minimizing operational effort while maintaining full detection capability.	
71	The solution must utilize Supervised Machine Learning models specifically trained on historical and real-world attacker behaviors (TTPs). The system must be capable of distinguishing between 'benign anomalies' (e.g., a software update or new admin activity) and 'malicious signals' (e.g., lateral movement or reconnaissance), ensuring that high-severity alerts are prioritized based on attack intent rather than simple statistical deviation	
72	The platform must extract and store enriched network metadata (not just NetFlow or PCAP) for a minimum of 30 days locally/on-cloud. This metadata must be indexed and searchable in real-time, allowing security analysts to perform retroactive 'Threat Hunting' queries across 40+ network protocols (including Kerberos, RPC, and DNS) without the need to replay raw packets.	
73	When suspicious activity is identified and alerted upon it is critical that the system provide appropriate commentary around the detection including appropriate triggers as well as steps to verify and where to begin potential remediation	
74	The solution must enrich it’s metadata/detections/hosts with the info that will help improve the IR approach, natively and without complex integrations (Host IID)	
75	The solution must provide unified entity attribution that correlates network metadata with identity-based signals (Active Directory/Azure AD) to maintain a persistent 'Threat & Certainty' score for a single user/host, even as they move across different IP addresses, VLANs, or hybrid-cloud environments	
76	In order for a fully effective deployment the solution must not requiring any third party object configuration changes (except for span/tap/mirror) such as adding additional locations for logging destinations.	
77	The solution must feature dedicated, non-signature-based AI models specifically trained to detect 'Hidden Command & Control (C2)' and 'Data Exfiltration' via HTTPS/DNS tunnels, with the ability to map these detections directly to specific MITRE ATT&CK techniques without requiring manual rule tuning	
78	The platform must utilize an automated prioritization engine that plots detections on a 2D quadrant of 'Threat Severity' vs. 'Certainty of Attack.' The solution must automatically surface only high-fidelity 'Critical' and 'High' quadrants for immediate SOC action, rather than a chronological list of all detected anomalies	
79	The proposed Network Detection and Response (NDR) solution must be capable of passively ingesting network traffic for analysis. This data ingestion shall be achieved by connecting to a network switch's Switch Port Analyzer (SPAN) or a network Test Access Port (TAP) at key points within the network infrastructure.	
80	Must be able to provide health monitoring via email and syslog.	

81	Must be able to alert on individual threats or suspicious hosts via email and syslog	
82	Must provide granular role-based access control (RBAC) into the various elements of the product so security analysts can define custom roles with limited access if desired	
83	Must have the ability to send audit log over syslog for actions such as login, logout and changes to settings that impact the security posture of the product	
84	The technology vendor should be NDR focused and must have at least 35 technology patents or higher	
85	The vendor must provide independent third-party validation (e.g., Gartner, MITRE ATT&CK Evaluations, peer-reviewed research, or equivalent) that supports the effectiveness of behavior-based detection of attacker techniques, not merely anomaly detection or reputation-based approaches.	

Signature: _____

Name: _____

Date: _____

Form F1

FINANCIAL PROPOSAL SUBMISSION FORM

[*Date*]

To:

Procurement Committee,
National Rural Support Programme,
IRM Complex, 7th Sunrise Avenue, Park Road,
Near COMSATS University, Islamabad.
Tel: (92-51) 8746170-73

Subject: Submission of Financial proposal RFP No. NRSP/FW/RQ-2634

Sir,

We, the undersigned, offer to provide the equipment & services for NRSP, in accordance with your Request for Proposal dated 4th August 2026. We are hereby submitting our Financial Proposal.

Our Proposal is binding upon us and subject to the modifications resulting from Contract negotiations. We understand that NRSP may accept or reject our proposal without giving any reason.

We understand you are not bound to accept any Proposal you receive.
We remain,

Yours sincerely,

Authorized Signature:
Name and Title of Signatory:
Name of Firm:
Address:
Email:
Contact No.:

Form F2

FINANCIAL PROPOSAL

S. No.	Description	Make/Model	Qty	Unit Price	Total Price
1	NDR with all Allied accessories		1		
2	Subscription & Technical OEM Support for 1 years 24//7/365		1		
3	Installation and Trainings		1 Job		
Sub Total:					
Sales Tax on Hardware					
Sales Tax on subscription & support licenses					
Sales Tax on installation & training					
Grand Total: (Including all charge and taxes)					

Validity of Proposal:

Delivery Time:

Bid Security Amount:

Any other details or terms & conditions: -

Signature: _____

Name: _____

Date: _____

Note: Pls attach the complete BOQ of the hardware in the financial proposal.

Annex-A

Code of Conduct and Ethics

(Non-Employee, consultants, vendors and third parties)

Upholding ethical standards protects the integrity, fairness, and transparency of the procurement process.

As a consultant/Vendor professional objective is to assist NRSP to add value to their enterprise, whether that enterprise takes the form of a business, a not-for-profit organization or any element of government.

As a consultant/vendor requires adherence to this Code of Conduct and Ethics as a condition of relation. All consultants/vendors have pledged to abide by the NRSP's Code of Conduct and Ethics and their voluntary adherence to the Code signifies the self-discipline of the profession.

All individuals (non-employees) contracted or functionally related to NRSP, including executing entities and third-party vendors: -

1. Will serve NRSP with integrity, competence, objectivity, independence and professionalism.
2. Will only accept assignments that they are competent to perform; and will only assign staff or engage colleagues with knowledge and expertise relevant to the assignment.
3. Before accepting any assignment will establish with NRSP realistic expectations of the objectives, scope, expected benefits, work plan and fee structure of the assignment.
4. Will treat all confidential NRSP information appropriately; will take reasonable steps to prevent access to confidential information by unauthorized people and will not take advantage of proprietary or privileged information, for use by them or others, without the NRSP's permission.
5. Will avoid conflicts of interest, or the appearance of such, and will disclose to NRSP immediately any circumstances or interests that they believe may influence their work, judgment or objectivity.
6. Will not contact NRSP during the any pre-solicitation or evaluation phase in which participated, unless NRSP contact for any information.
7. Will offer to withdraw from assignment when they believe their objectivity or integrity may be impaired.
8. Will inform NRSP immediately if there is any change is contact person, email, address, directors, release of any of his/her employee or any such information which could be necessary for NRSP record.
9. Will represent the profession with integrity and professionalism in their relations with NRSP, colleagues and the general public.
10. Will report to appropriate authorities within or external to NRSP organization any occurrences of malfeasance, dangerous behavior or illegal activities discovered during the course of an assignment.
11. Will not offer commissions, gift, bribe, remuneration, or other benefits from himself or from a third party in connection with any assignment to NRSP, and will disclose in advance any financial interests.
12. Will promote adherence to the Code of Conduct and Ethics by all other staff working on their behalf.
13. Strive to treat all persons of NRSP with respect and courtesy in accordance with applicable international and national conventions and standards of behavior;
14. Never intentionally commit any act or omission that could result in physical, sexual or psychological harm to the beneficiaries we serve, or to their fellow workers;
15. Not condone or intentionally participate in corrupt activities or illegal activities. While respecting and adhering to these broader frameworks of behavior,
16. Shall not harass, discriminate, or retaliate against any other consultant/vendor or any member of society.
17. Shall make themselves available and fully participate in all administrative inquiries with completely honesty.
18. No NRSP employees shall solicit anything of value from a citizen or business for services that the NRSP is expected to provide.
19. Shall not remove NRSP property from its assigned place for personal use. Defacing or destroying NRSP property is vandalism and shall be dealt strictly.
20. Will not permit considerations of race, gender, nationality, religion, politics, sexual orientation or social status to influence professional behavior or advice.
21. Will be respectful of those whose wellbeing may be contingent. Will diligently apply objective judgment to all consulting assignments, based on the best information available. Will conduct independent research and analysis where possible, and will consult with colleagues and others who can help inform the judgment.
22. Will not use any services, goods, materials, technology and/or equipment provided by or paid for by NRSP for illegal, inappropriate, or otherwise disruptive activities, or in support of such activities.
23. Shall not place or display non-official notices in NRSP premises without prior written approval from the appropriate authority.
24. Shall not possess unauthorized weapons, illegal drugs, or alcohol on NRSP premises.
25. Shall strictly follow the NRSP's workplace policies while on any NRSP premises.
26. Will uphold NRSP's commitment to gender equality, non-discrimination, and the prevention of Sexual Exploitation, Abuse, and Harassment (SEAH) at all times in the course of their work.
27. Will maintain a working environment that is free from all forms of SEAH& gender-based violence, in alignment with NRSP's Gender Mainstreaming Policy.

This Code of conduct is not exhaustive and may not anticipate every situation which may morally, ethically, professionally, legally compromise the employees or NRSP interests. In this regard NRSP expects to use sound judgment. However, compliance with this Code is a mandatory obligation owed by all consultants, third party vendors etc. Breach of this Code or any requirements mentioned in these Rules will result in disciplinary action and may lead up to cancellation of work order/registration including legal action or other appropriate disciplinary actions.

Anti-Money Laundering and Anti-Terrorism Financing Policy

Policy

"It is the policy of the NRSP to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorism or criminal activities" by complying with all applicable requirements under the **Anti-Money Laundering Act 2010** (Act No. VII of 2010 - an Act to provide for prevention of money laundering) and **Anti-Terrorism (Second Amendment) Act, 2014** and its implementation regulations. Recently under the national action plan and SECP regulations money laundering has been identified as a major cause for corruption and criminal activities. Therefore, NRSP is very sensitive to ensuring that our platform is not used for any such purposes.
