NRSP

National Rural Support Programme

National Rural Support Programme
IRM Complex, 7, Sunrise Avenue, Park Road, Chak Shehzad,
Near COMSATS University, Islamabad. Ph: +92-51-8746170-3

Date: June 03, 2022

Tender No. NRSP/SIEM Software and Server Hardware EQUIPMENT /RQ-677

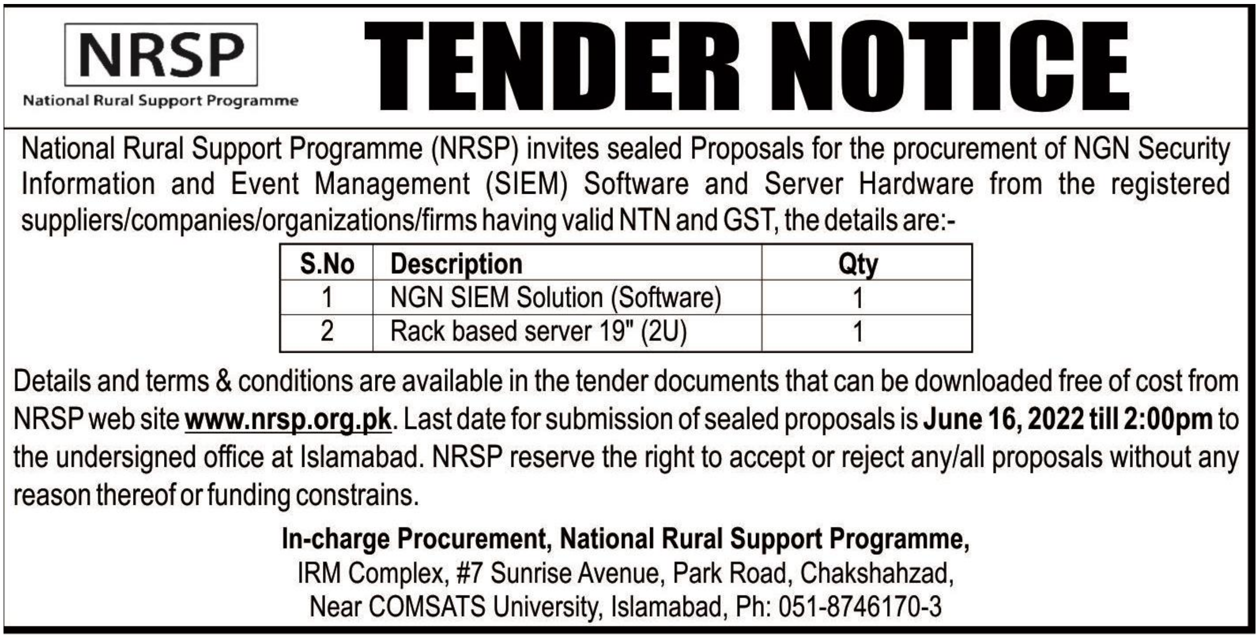
Tender documents for the purchase of

Security Information and Event Management (SIEM) Software and Hardware

for

National Rural Support Programme (NRSP)

NEWSPAPER ADVERTISMENT



NRSP

National Rural Support Programme

TENDER NOTICE

National Rural Support Programme (NRSP) invites sealed Proposals for the procurement of NGN Security Information and Event Management (SIEM) Software and Server Hardware from the registered suppliers/companies/organizations/firms having valid NTN and GST, the details are:-

S.No	Description	Qty
1	NGN SIEM Solution (Software)	1
2	Rack based server 19" (2U)	1

Details and terms & conditions are available in the tender documents that can be downloaded free of cost from NRSP web site **www.nrsp.org.pk**. Last date for submission of sealed proposals is **June 16, 2022 till 2:00pm** to the undersigned office at Islamabad. NRSP reserve the right to accept or reject any/all proposals without any reason thereof or funding constrains.

In-charge Procurement, National Rural Support Programme,
IRM Complex, #7 Sunrise Avenue, Park Road, Chakshahzad,
Near COMSATS University, Islamabad, Ph: 051-8746170-3

Published on June 03, 2022 in Daily The Nawa-e-Waqat (Lahore/Karachi Editions),
Daily The News (Rwp-Isd Edition).

Details		
1.	Date of availability of tender documents(RFP) on NRSP website	**June 03, 2022**
2.	Last date and time for sending queries/question or clarifications by suppliers	**June 07, 2022**
3.	Last date and time for reply of queries/question or clarifications by NRSP	**June 09, 2022**
4.	Last date, time and address for receipt of Tender Documents/Proposals (in hard copies)	**June 16, 2022 by 2:00 p.m.(PST)** 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	**June 16, 2022 by2:30p.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 Suppliers	Interested Suppliers are requested to send their queries on the following email: procurement@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 event.

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 branch network so there is need to upgrade its existing hardware for better security and performance. The detail specification of the required networking hardware are given in section 3.

3. Procurement details.

The project scope spans around NRSP Islamabad datacenter. The selected supplier will supply, install, configure, test & maintain the Next generation Security Information and Event management (SIEM) software and Server hardware equipment. The selected supplier will also be responsible for integrating the newly installed Next generation SIEM software and Server hardware with existing server farm infrastructure and datacenter network. The selected supplier 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 supplier during contract period.

The successful supplier will be responsible for:

a) Supply of server hardware and SIEM Software
b) Complete Installation/Commissioning of SIEM software & related configurations.
c) Smooth and timely User Acceptance Test
d) Project management for supply of goods, support, warranty and services for the entire project.

Below is the complete list of SIEM software and server hardware to be purchased under this tender.

S.No.	Software/Hardware	Details
01	**NGN SIEM Solution (Software)**	**1 Log Management** **1.1 Platform** 1.1.1 The Platform must include log management, NG SIEM, Host Forensics, UEBA, NDR, File Integrity Monitoring, Security Analytics, Security Automation and Orchestration engine (includes but not limited to Incident Management, Incident

		Response), Advanced Correlation within the same platform with no additional 3rd party solution) 1.1.2 Provide a full list of systems, applications, and devices supported as identified log sources list with fully developed normalization logic out-of-the-box by the solution. 1.1.3 Describe out-of-the-box content provided with the solution. Detail the number of: supported devices, rules, reports, searches, modules, report packages, alarms, lists, dashboards, threat feeds integrations, etc. 1.1.4 The proposed solution must support active/active cluster for scalability purposes, up to 10 appliances in a single cluster with the capability to build multiple of clusters and manage all of them from the same centralized interface 1.1.5 The Proposed Solution must offer all of the below built-in modules out of the box at no additional cost: Advanced Threat Detection Modules • Network Detection and Response Module • Fraud Detection Module • User and Entity Behavioral Analytics Module • User Threat Defense • Endpoint Threat Defense • MITRE ATT&CK module Compliance Modules • GLBA Compliance Module • FISMA Compliance Module • GPG-13 Compliance Module • PCI-DSS Compliance Module • BSI IT-Grundschutz Module • 201 CMR 17 Module

		• HIPAA Module • NERC-CIP Module • ASD Module • SOX Module • HiTech Module • Dodi 8500.2 Module • NRC Module • NEI Module • CCF Module • GDPR Compliance Module • ISO Compliance Module • Network Detection and Response Module • Fraud Detection Module • User and Entity Behavioral Analytics Module • User Threat Defense • Endpoint Threat Defense • MITRE ATT&CK module • UAE NESA Compliance Package • KSA Essential Cybersecurity Controls Compliance Package 1.1.6 The solution must support very granular level of role-based access.: • Allow different teams to get an access to the same physical device and view date related to their department only

- It must support log source visualization on the SIEM platform itself

1.2 Log Collection

1.2.1 The Proposed solution must collect the logs in real-time and batch mode

1.2.2 The proposed solution must correct event time for logs from systems with incorrect timestamps. Also, describe how the platform handles logs configured with different time zones.

1.2.3 The proposed solution must support the options for scheduling delivery, compressing, and/or encrypting remotely collected log data; in addition to the ability to filter out and drop some noisy logs at the collection layer before it reaches to the processing and indexing engine.

1.2.4 The data collector/agent must be able to collect the logs through different methods, including but not limited to:

- UDP/TCP Syslog
- SNMP
- Cisco SDEE
- NetFlow
- JFlow
- Sflow
- Universal Database Log Adapter for system and custom logs (e.g., audit, application, etc.) written to database tables (i.e. Oracle, SQL Server, MYSQL, etc.) (ODBC and OLE DB protocol)
- Checkpoint OPSEC/LEA
- AS/400 and iSeries (can be via 3rd party integration)
- Windows Event Logs (RPC) - this includes custom Event Logs (by using RPC not WMI).

		• Windows Event Logs (local) – this includes custom Event logs • Single-line Flat Files • Multi-line Flat Files • Compressed Flat Files (single and multi-line) • NetApp CIFS • eStreamer • Metasploit • Nexpose • Nessus • eEye Retina • Qualys • Tripwire • API • JSON format 1.2.5 The proposed solution collector must support the automatic load balancing, load sharing, secure the communication during the log collection mechanism, and collect the logs through an agent-less and agent based if required. 1.2.6 The proposed solution must support the ability to scan a Windows domain to automate discovery and event collection from windows hosts. 1.2.7 The proposed solution must support Windows Event log collection for Security, System, and Application events. Describe the process of ingesting and normalizing windows logs for search, correlation, alerting, reporting, etc. How often updates are provided to Windows Event normalization rules.

1.2.8 The proposed solution must allow log collection to be continue in the event communication with the back-end platform is temporarily interrupted. The solution also must include alerting mechanism that can be easily configured if a log source stops sending log data

1.2.9 The proposed solution must support the collection of the Net flow logs.

1.3 File Integrity Monitoring

1.3.1 The proposed solution should optionally provide integrated built-in File Integrity Monitoring (FIM) not through a 3rd party software and it should be managed and monitored by the same NG-SIEM platform interface.

1.3.2 The proposed solution File Integrity Monitoring capability must be able to capture the identity of the user generating the FIM events, and support for both Windows and *Nix platforms.

1.3.3 The proposed solution built-in FIM must pivot from a file access or change to a specific user. View a full timeline of their activity, including both file integrity monitoring (FIM) and other behavioral information

1.3.4 The prosed solution built-in FIM must selectively monitor file views, modifications and deletions, and modifications, as well as group, owner and permissions changes

1.3.5 The proposed solution built-in FIM must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data

1.4 Log Retention

1.4.1 The proposed solution must store the raw logs and also the meta-data consistently.

1.4.2 The proposed solution must compress the archive logs and provide hashing capability on archive files to ensure log data integrity

1.4.3 The proposed solution must utilize any storage methodologies for addressing different ages of log or event data (e.g. hot vs. cold storage)

1.4.4 The proposed solution must provide storage for long term trend visualization and analysis

2 Analytics

2.1 Log Analysis

2.1.1 The proposed solution must analyze the logs in real time.

2.1.2 The proposed solution must support multiple layers of log classification and categorization by default and out-of-the-box. For example:

- Layer 1: Audit – Operations - Security.
- Layer 2: Classification subcategories.
- Layer 3: Common Event types under each classification.
- Layer 4: Utilized Normalization Rules for better events analysis and visualization.

2.1.3 Describe data enrichment capabilities, including the number and type of available fields.

2.1.4 The proposed solution must represent large search results in a single view

2.1.5 The proposed solution must perform geo location to IP addresses

2.1.6 The proposed solution must perform DNS resolution for IP addresses

2.1.7 Describe the real-time visualization options, features and capabilities of the dashboard.

2.1.8 The proposed solution must allow for the easy creation of custom dashboards. The dashboard views be saved and shared among groups specific to a use case such as a Security Analyst or IT Operations

2.1.9 The proposed solution must contextualize the user information with a detailed information about the user attributes from the domain such as username, title, department, last time to log on, last time he failed in the password, email address...etc.

2.1.10 The platform must have the capability to apply security and operational analytics

2.2 Real-Time Advanced Analytics

2.2.1 Please mention, in quantities, the below supported out-of-the-box capabilities:

- Data Classification types and sub-classification types
- Common event types available for data identification
- Log Messages Processing Engine Rules (Parsing Rules)
- Predefined Use Cases
- Predefined Reports

2.2.2 The proposed solution alarms and searches must be unlimited functionalities and not limited functionalities, for example by the size of the deployment, such as by the number of available CPU cores.

2.2.3 The proposed solution must employ advanced intelligence analytics.

2.2.4 The proposed solution must perform advanced analytics against all log data or a subset of the data.

2.2.5 The proposed solution must have a risk based priority engine that can assign a risk value for all the logs, events and alarms natively at no additional cost

2.2.6 The proposed solution must automatically determine threats based on suspicious patterns of behavior.

2.2.7 The proposed solution must have the ability to automatically create whitelists of observed behavior (i.e. without manual intervention)

		2.2.8 The proposed solution must have the ability to automatically learn behavioral or statistical baselines. 2.2.9 The proposed solution must offer the U.E.B.A natively out of the box. 2.2.10 The proposed solution must have the ability to leverage correlated or anomaly events back into other correlation or advanced analytics rules. 2.2.11 The proposed solution must incorporate data from multiple threat intelligence feeds into its’ advanced analytics. 2.2.12 The proposed solution must provide updated analytics rules on a regular basis to detect new and emerging threats. 2.2.13 The proposed solution must allow the organization to build a filter and reuse it with multiple of correlation rules 2.2.14 The solution must support many different types of correlation and analytics methods: • Log: • Log Observed based correlation. • Non-Observed Compound based correlation. • Non-Observed Scheduled based correlation. • Session sequence based correlation. • Threshold: • Threshold observed based correlation. • Threshold non-observed compound based correlation. • Threshold non-observed scheduled based correlation. • Unique Value: • Unique value observed based correlation. • Unique value non-observed compound based correlation. • Unique values non-observed scheduled based correlation • Behavioral: • Whitelist based correlation.

- Blacklist based correlation.
- Machine analytics based correlation.
- Statistical based correlation.
- Trend based correlation

2.3 Event Response and Alerting

2.3.1 The proposed solution must provide an ability to interface with a third-party incident response management system (e.g. Remedy, etc.)

2.3.2 The proposed solution must provide out-of-the-box alarms designed to enforce continuous compliance and security best practices

2.3.3 The proposed solution must provide the ability to create customized alarms, distributed to specific groups of individuals and prioritize alarms and alarm delivery.

2.3.4 The proposed solution must email alarm notifications include risk rating priority level. With configurable alarm email subject line.

3 UEBA

- The UEBA must be offered Fully Integrated within the proposed solution.
- The UEBA shouldn’t be limited to the number of users.
- The UEBA must be able to detect and respond to insider threats, compromised account, and privileged account abuse
- The UEBA must collect machine data from across your environment and fill in your forensic gaps with endpoint and network monitoring
- The UEBA must correlate log information to single identities to know the actors behind the actions impacting your environment with Identity Inference, which attributes identities to anonymous log messages, streamlining forensic investigations

- The UEBA must Detect threats of data exfiltration, privileged identity misuse and fraud
- The proposed solution must share the list of predefined out of the box use cases related to UEBA

•The platform must have a list of use cases out-of-the-box and should have the ability to customize or build from scratch. Please explain how many out-of-the-box use cases are supported by the solution.

Host Forensics

The proposed solution should have an optional agent that can achieve the following:

- File Integrity Monitoring
- Process activity monitoring
- Network Communication Monitoring
- Registry keys Integrity Monitoring
- Data loss defender
- User Activity Monitoring

Administration

Ease of Use

4.1.1 Describe support for centralized administration in a geographically dispersed deployment.

4.1.2 The solution should provide centralized health monitoring of itself.

4.1.3 There must be wizards available to guide administrators through any of the administration processes.

Reporting

5.1.1 The proposed solution must offer all the reports out of the box at no additional cost.

5.1.2 The solution must include pre-defined reports.

5.1.3 Reports must be scheduled and delivered to the recipients in an automated manner. Reports must be restricted to different levels of management within the company.

			5.1.4 It must have a rest API to allow 3rd party tool to query and report the logs such as Kibana for instance.
02	**1xRack based Server 19" (2U)**	**CPU**	2xIntel® Xeon® Gold 5317 (12C, 3.0 GHz, TLC: 18 MB, Turbo: 3.40 GHz, 11.2 GT/s,
		Memory	8x32GB (1x32GB) 2Rx4 DDR4-3200 R ECC
		Disk	16xHD SAS 12G 1.2TB 10K 512n HOT PL 2.5' EP
			4xSSD SATA 6Gbs 480 GB
		Raid Controller	1xPRAID EP680i LP SAS/SATA/PCIE-NVMe RAID Controller based on LSI Mega RAID SAS3916 - for up to 16 internal SAS/SATA HDD, SSD, for mixed configuration SAS, SATA and up to 2 times x4 PCIe-NVMe SSD - RAID Levels 0, 1, 10, 5, 50, 6, 60 - TFM already included - 8GB Cache - Safe Store and Fast Path included - Cache Cade® not any longer supported
		Lan	**Lan 1**: 2x10GBASE-T PCIE LP **Lan 2**: 4x1Gbit
		PSU	2x900W modular Power Supply Module ,
		Rack Mount Kit	2xRack Mount Kit (RMK) for server max.
		Power Cord	2xCable power cord rack, 1.8m, black Power cord for rack mounting+, IEC 320 C14 -> C13 (10A plug), 1.8m
		System Management	iRMC advanced pack (Remote Graphical Console)
		Warranty	Standard Warranty 3 years
03	**Training**	Professional level class room and hands on training by principal only.	

4. Requirements

1. Proposed SIEM software & hardware must be in Leaders of Magic Quadrant of Gartner of July, 2021.
2. The proposed software and hardware market launch date should not be before 2020.
3. To provide the offered product roadmap for next 5 years (2022 onwards).
4. Installation and configurations with respect to NRSP Network design and NRSP Business requirements.
5. The supplier should provide a plan for Support, Warranty and Services in its technical proposal.
6. 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.

7. 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 in this RFP. (Refer to Form E1)

5.1 Must be registered with SECP/ Registrar of Firms in Pakistan and working for the last 10 years in Pakistan in the field of IT (Certificate of Incorporation to be attached from SECP/Registrar of Firms).

5.2 Supplier must have 3 years' experience in selling SIEM software and Hardware equipment (attach valid proofs in the shape of orders or completion certificates).

5.3 Supplier must be authorized dealer of the proposed software and hardware. The supplier must provide Manufacturer Authorization Letter (MAL) with reference to this tender to participate in this tender.

5.4 Supplier must have successfully provided offered software and hardware to at least five clients in Pakistan (attach valid proofs in the shape of completion certificate with complete contact details, PO will not be taken as proof).

5.5 Supplier must have at least three certified professionals from OEM of proposed software and hardware to support the offered equipment (attach updated current CVs of the certified professional with copies of relevant valid certificates).

5.6 Undertaking of blacklisting as per Form E1.1

6 Submission of Proposals

Proposals will be accepted and evaluated using **Single Stage – Two Envelop Procedure**, The Technical and Financial proposals shall be submitted on the same day but in a separate sealed envelope clearly mentioned Technical and Financial Proposals marked as:-

Technical Proposal - Tender No. NRSP/SIEM Software and Server Hardware EQUIPMENT /RQ-677

&

Financial Proposal – Tender No. NRSP/SIEM Software and Server Hardware EQUIPMENT /RQ-677

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

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

a. Technical Proposal Submission Form (Form T1)
b. Mandatory Eligibility Criteria (Form E1)
c. Company Profile. (Form T2)
d. Specific experience for similar assignments (Form T3).
e. General experience (Form T4).
f. Qualification and Competence of the proposed team for support for this assignment (From T5)
g. Proposed software and hardware compliance with required specifications, delivery time, installation/testing/commissioning plan (Form T6)

h. Proposed Software and Hardware with make and model/version, SLA details, Subscription & Support details and training details. All the relevant literature, catalogs, data sheets, Gartner rating document, brouchers must be attached showing the technical specifications in details with technical compliance sheet.

i. Any other document which could be helpful in the technical evaluation.
The technical proposal shall not include any financial information.

6.2 The **financial proposal** shall contain the following information:

a. Financial Proposal Submission Form (Form F1)

b. The DDP (Ex-Islamabad NRSP Data Center) price of each item with complete details, make and model. All applicable taxes and mentioned clearly. Prices should be on DDP (NRSP Data Center, Sihala), Islamabad basis. (Form F2)

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

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

e. Bid Security @2% of the total deliverable in the shape of Call deposit/Pay Order/Demand Draft/cashier cheque in the name of NRSP.

f. Validity of the financial proposal.

g. Other terms and conditions (if any).

6.3 Suppliers must offer all the software and hardware with training as given in section 3. Incomplete or partial tenders will be rejected.

6.4 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.

6.5 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 of the suppliers, for which the concerned supplier will need to submit the documentary evidence(s) as required by NRSP.

6.6 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, he may be debarred from participation in the future tendering processes.

6.7 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.

6.8 **Last Date of Submission is June 16, 2022 till 2:00 pm local time.**

6.9 The proposals must be submitted in original hard copy not later than June 16, 2022 till 2:00pm 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.

6.10 The proposals should be marked/addressed as:

(Proposal for NGN SIEM Software and Hardware for NRSP)
Tender No. NRSP/SIEM Software and Server Hardware EQUIPMENT /RQ-677
Procurement Committee
National Rural Support Programme
IRM Complex, 7, Sunrise Avenue, Park Road, Chak Shehzad,
Near COMSATS University, Islamabad.
Ph:+92-51-8746170-3.

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

6.12 The offer should remain valid for a period of **60 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.

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

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

6.15 Selected supplier must undertake to provide NRSP, the consignment note 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.

6.16 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

Final evaluation of the proposal will be carried by using the below combination.

S.NO.	PROPOSAL	WEIGHT
1	Technical	70%
2	Financial	30%
	TOTAL	**100%**

Following is the scoring criteria for Technical & Financial Evaluation.

7.1 Technical Evaluation

S. No	Description	Max Marks	Remarks		Min Marks
1	Company Profile	15	Established and working for more than 10 years	15	10
			Established and working upto 10 years	10	
2	Level of partnership with OEM for software and hardware	25	Highest Level	20	15
			Other than highest level	15	
3	Technical Team	20	More than 10 members	20	10
			More than 5 member and less than 10 members	15	

			More than 3 member and less than 5 members	10	
4	Clients to whom the proposed type of software and hardware	30	Supplied to more than 05 clients	30	15
			Supplied upto 05 clients	15	
5	Compliance to Technical requirements	10	Meets the technical requirements	10	10
			Does not meet the technical requirements	0	

Note: Failure to score minimum marks in each section will result disqualification technically.

7.2 Financial Evaluation

S. No.	Financial Evaluation	Marks
a.	Lowest Bid Price	30
TOTAL POINTS		**30**

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, ask some or all suppliers for clarification of their offer. The request for such clarifications and the response will necessarily be in writing.

8 Selection Process

A selection committee from NRSP will evaluate the technical proposals which are eligible as per clause 5 and assign score to each technical proposal according to above details. To qualify technically a minimum score of 60 is needed. Financial Proposals will be opened of only those suppliers whose technical proposal are qualified. Financial proposal of those suppliers who are not technically qualified will be returned un-opened. Financial proposals will also be opened in the presence of suppliers for which the date will be announced after the technical evaluation. Supplier scoring the highest marks (Technical + Financial) will be selected for the award of the contract. This process should normally take about 15 50 20 days.

9 Deliverables

Networking equipment and trainings as per details given section 3.

10 Terms of Proposal

10.1 Bid Security

All suppliers shall furnish Bid Security Deposit equivalent to **2% of the total Cost of Deliverables** in the form of Call deposit/Pay Order/Demand Draft/cashier cheque 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.

10.2 **Performance Security**

Performance security will be 10% of the total cost of the Software and Hardware (excluding training) which will be withheld from the final payment for the period of three year. After the successful completion of warranty period of three years, performance security will be released.

11 Fees and payment Schedule

11.1 No Advance will be allowed in any case.

11.2 Payment will be made after the complete and satisfactory delivery/acceptance/testing/ configuration of the software, hardware and training to the designated delivery site/destinations within 2-3 weeks through cross cheque.

11.3 Partial delivery and partial payment allowed.

11.4 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.

12 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/installation report.

13 Delivery Schedule

13.1 The Selected supplier must undertake to deliver the equipment ordered, to NRSP Data Center Sihala Islamabad 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.

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

14 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 equipment. All the hardware should have one year warranty from the date of supply/installation as mentioned in the section 3.

15 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.

16 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.

17 Currency

All prices shall be expressed in Pakistani Rupees only.

18 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 bidding process.

19 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.

20 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 bids 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.

21 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.

22 General Terms & Conditions

22.1 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.

22.2 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.

22.3 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.

22.4 Canvassing of any kind will be a disqualification and the NRSP may decide to cancel the supplier from its empanelment.

22.5 Supplier code of conduct is attached for required compliance as Annex A.

23 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 Telegram/Fax/E-mail.
c. If the proposal is submitted without or less or not in required type the bid security deposit.
d. If the technical bid 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.
f. 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.

24 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.

25 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 Tender document at the address mentioned at bidding details.
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 satisfying the technical requirements as determined by NRSP 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, third supplier etc. if successful supplier is not able to supply the deliverables and his bid security will be forfeited.

26 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.

27 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 bidding 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.

28 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.

29 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.

30 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.

31 Appeals

Suppliers believing that they have been harmed by an error or irregularity during the award process may file a complaint to NRSP at complaints@nrsp.org.pk.

STANDARD FORMS

Form E1

(To be submitted on firm/company letter head)

	MANDATORY ELIGIBILITY CRITERIA	Yes	No
1	Must be registered with SECP/ Registrar of Firms in Pakistan and working for the last 10 years in Pakistan in the field of IT (Certificate of Incorporation to be attached from SECP/Registrar of Firms).	□	□
2	Supplier must have at least 3 years' experience in selling proposed type of hardware. (Attach documentary evidence in shape or orders/contracts/completion certificates)	□	□
3	Supplier must be authorized dealer of the proposed software and hardware. The supplier must provide Manufacturer Authorization Letter (MAL) with reference to this tender to participate in this tender.	□	□
4	Supplier must have successfully provided offered software and hardware to at least five clients in Pakistan (attach valid proofs in the shape of completion certificate with complete contact details, PO will not be taken as proof).	□	□
5	Supplier must have at least three certified professionals from OEM of proposed software and hardware to support the offered equipment (attach updated current CVs of the certified professional with copies of relevant valid certificates).	□	□
6	Affidavit (on Rs.100/- stamp paper) dully signed and attested by Notary public as per format provided in From E1.1	□	□

Authorized Signature: ________________________
Stamp: _____________________________________
Date: ______________________________________

Form E1.1

UNDERTAKING/DECLARATION OF ELIGIBILITY

In the response to your Tender No. NRSP/SIEM Software and Server Hardware EQUIPMENT /RQ-677**,** I/We, the undersigned, hereby declare that:

- Our proposal is valid for a period of 60 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 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.
- 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 witness and attested by Notary public)

Form T1

(To be submitted on firm/company letter head)

TECHNICAL PROPOSAL SUBMISSION FORM

[Location, 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 Tender No. NRSP/SIEM Software and Server Hardware EQUIPMENT /RQ-677

Sir,

We, the undersigned, offer to provide the equipment & services to NRSP, in accordance with your subject tender. 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 Cell No.:

Form T2

(To be submitted on firm/company letter head)

FIRM PROFILE

S #	Criteria	Details /Remarks
1	Profile of the supplier: i. Registration details and age of Company ii. Names of Managers/ Owners/ CEO/ Directors/ Partners with CNIC	
2	Location of supplier office/sub office Number of branches Number of employees	
3	Financial Position i. Name of Bank(s) ii. Certificate of Financial position from bank(s) iii. Copy of last financial year audit report dully signed by the auditor iv. Tax Registration (copies of NTN & STN)	

Authorized Signature: ______________________

Stamp: __________________________________

Date: ___________________________________

Form T3

(To be submitted on firm/company letter head)

SPECIFIC EXPERIENCE FOR SUPPLY OF PROPOASED TYPE OF SOFTWARE AND HARDWARE

NAME OF CLIENT(S)	NAME OF ASSIGNMENT/ PROJECT	PERIOD OF ASSIGNMENT/ PROJECT	VALUE OF ASSIGNEMNT / PROJECT	CONTACT DETAILS OF CLIENT

Authorized Signature: ______________________
Stamp: __________________________________
Date: ___________________________________

Form T4

(To be submitted on firm/company letter head)

GENERAL EXPERIENCE OF SUPPLIER

NAME OF CLIENT	NAME OF ASSIGNMENT/ PROJECT	PERIOD OF ASSIGNMENT/ PROJECT	VALUE OF ASSIGNEMNT / PROJECT	PRESENT STATUS OF THE ASSIGNMENT/ PROJECT

Authorized Signature: ________________________
Stamp: _____________________________________
Date: ______________________________________

Form T5

(To be submitted on firm/company letter head)

QUALIFICATION AND COMPETENCE OF PROPOSED TEAM FOR SUPPORT FOR THIS ASSIGNMENT

Personnel Summary (Complete for each Team Member)

Name of Employee:		
Position		
General Information	Name:	Date of Birth:
	Telephone:	
	Cell No.:	
	Years with Present Employer:	

Employment Record:

Summarize professional experience in reverse chronological order. Indicate particular technical and managerial experience relevant to the project:

DD/MM/YY		**Company/Project/Position/Specific Tech experience**
From	**To**	

Education:

Highest Level of Degree	**Relevance of Degree to the Assignment**

PhD	
MPhil	
Masters	
Other	

Certification:

Name of course/certificate	**Brief description**

Undertaking:

I, the undersigned, certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience.

____Date: _____________

[Signature of staff member and authorized representative of the firm] *Day/Month/Year*

Full name of staff member: ______________________________________

Authorized Signature: ________________________
Stamp: _____________________________________
Date: ______________________________________

Form T6

(To be submitted on firm/company letter head)

PROPOSED SOFTWAR AND HARDWARE COMPLIANCE SHEET WITH SPECIFICATIONS, DELIVERY TIME AND WORKPLAN.

Software/Hardware	Details	Yes	No
NGN SIEM Solution	1 Log Management 1.1 Platform 1.1.1 The Platform must include log management, NG SIEM, Host Forensics, UEBA, NDR, File Integrity Monitoring, Security Analytics, Security Automation and Orchestration engine (includes but not limited to Incident Management, Incident Response), Advanced Correlation within the same platform with no additional 3rd party solution) 1.1.2 Provide a full list of systems, applications, and devices supported as identified log sources list with fully developed normalization logic out-of-the-box by the solution. 1.1.3 Describe out-of-the-box content provided with the solution. Detail the number of: supported devices, rules, reports, searches, modules, report packages, alarms, lists, dashboards, threat feeds integrations, etc. 1.1.4 The proposed solution must support active/active cluster for scalability purposes, up to 10 appliances in a single cluster with the capability to build multiple of clusters and manage all of them from the same centralized interface 1.1.5 The Proposed Solution must offer all of the below built-in modules out of the box at no additional cost: Advanced Threat Detection Modules		

	• Network Detection and Response Module • Fraud Detection Module • User and Entity Behavioral Analytics Module • User Threat Defense • Endpoint Threat Defense • MITRE ATT&CK module Compliance Modules • GLBA Compliance Module • FISMA Compliance Module • GPG-13 Compliance Module • PCI-DSS Compliance Module • BSI IT-Grundschutz Module • 201 CMR 17 Module • HIPAA Module • NERC-CIP Module • ASD Module • SOX Module • HiTech Module • Dodi 8500.2 Module • NRC Module • NEI Module • CCF Module • GDPR Compliance Module • ISO Compliance Module		

- Network Detection and Response Module
- Fraud Detection Module
- User and Entity Behavioral Analytics Module
- User Threat Defense
- Endpoint Threat Defense
- MITRE ATT&CK module
- UAE NESA Compliance Package
- KSA Essential Cybersecurity Controls Compliance Package

1.1.6 The solution must support very granular level of role-based access.:

- Allow different teams to get an access to the same physical device and view date related to their department only
- It must support log source visualization on the SIEM platform itself

1.2 Log Collection

1.2.1 The Proposed solution must collect the logs in real-time and batch mode

1.2.2 The proposed solution must correct event time for logs from systems with incorrect timestamps. Also, describe how the platform handles logs configured with different time zones.

1.2.3 The proposed solution must support the options for scheduling delivery, compressing, and/or encrypting remotely collected log data; in addition to the ability to filter out and drop

	some noisy logs at the collection layer before it reaches to the processing and indexing engine. 1.2.4 The data collector/agent must be able to collect the logs through different methods, including but not limited to: • UDP/TCP Syslog • SNMP • Cisco SDEE • NetFlow • JFlow • Sflow • Universal Database Log Adapter for system and custom logs (e.g., audit, application, etc.) written to database tables (i.e. Oracle, SQL Server, MYSQL, etc.) (ODBC and OLE DB protocol) • Checkpoint OPSEC/LEA • AS/400 and iSeries (can be via 3rd party integration) • Windows Event Logs (RPC) - this includes custom Event Logs (by using RPC not WMI). • Windows Event Logs (local) – this includes custom Event logs • Single-line Flat Files • Multi-line Flat Files • Compressed Flat Files (single and multi-line) • NetApp CIFS		

	• eStreamer • Metasploit • Nexpose • Nessus • eEye Retina • Qualys • Tripwire • API • JSON format 1.2.5 The proposed solution collector must support the automatic load balancing, load sharing, secure the communication during the log collection mechanism, and collect the logs through an agent-less and agent based if required. 1.2.6 The proposed solution must support the ability to scan a Windows domain to automate discovery and event collection from windows hosts. 1.2.7 The proposed solution must support Windows Event log collection for Security, System, and Application events. Describe the process of ingesting and normalizing windows logs for search, correlation, alerting, reporting, etc. How often updates are provided to Windows Event normalization rules. 1.2.8 The proposed solution must allow log collection to be continue in the event communication with the back-end platform is temporarily interrupted. The solution also must include		

	alerting mechanism that can be easily configured if a log source stops sending log data 1.2.9 The proposed solution must support the collection of the Net flow logs. **1.3 File Integrity Monitoring** 1.3.1 The proposed solution should optionally provide integrated built-in File Integrity Monitoring (FIM) not through a 3rd party software and it should be managed and monitored by the same NG-SIEM platform interface. 1.3.2 The proposed solution File Integrity Monitoring capability must be able to capture the identity of the user generating the FIM events, and support for both Windows and *Nix platforms. 1.3.3 The proposed solution built-in FIM must pivot from a file access or change to a specific user. View a full timeline of their activity, including both file integrity monitoring (FIM) and other behavioral information 1.3.4 The prosed solution built-in FIM must selectively monitor file views, modifications and deletions, and modifications, as well as group, owner and permissions changes 1.3.5 The proposed solution built-in FIM must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data **1.4 Log Retention** 1.4.1 The proposed solution must store the raw logs and also the meta-data consistently.		

1.4.2 The proposed solution must compress the archive logs and provide hashing capability on archive files to ensure log data integrity

1.4.3 The proposed solution must utilize any storage methodologies for addressing different ages of log or event data (e.g. hot vs. cold storage)

1.4.4 The proposed solution must provide storage for long term trend visualization and analysis

2 Analytics

2.1 Log Analysis

2.1.1 The proposed solution must analyze the logs in real time.

2.1.2 The proposed solution must support multiple layers of log classification and categorization by default and out-of-the-box. For example:

- Layer 1: Audit – Operations - Security.
- Layer 2: Classification subcategories.
- Layer 3: Common Event types under each classification.
- Layer 4: Utilized Normalization Rules for better events analysis and visualization.

2.1.3 Describe data enrichment capabilities, including the number and type of available fields.

2.1.4 The proposed solution must represent large search results in a single view

2.1.5 The proposed solution must perform geo location to IP addresses

2.1.6 The proposed solution must perform DNS resolution for IP addresses

	2.1.7 Describe the real-time visualization options, features and capabilities of the dashboard. 2.1.8 The proposed solution must allow for the easy creation of custom dashboards. The dashboard views be saved and shared among groups specific to a use case such as a Security Analyst or IT Operations 2.1.9 The proposed solution must contextualize the user information with a detailed information about the user attributes from the domain such as username, title, department, last time to log on, last time he failed in the password, email address...etc. 2.1.10 The platform must have the capability to apply security and operational analytics **2.2 Real-Time Advanced Analytics** 2.2.1 Please mention, in quantities, the below supported out-of-the-box capabilities: • Data Classification types and sub-classification types • Common event types available for data identification • Log Messages Processing Engine Rules (Parsing Rules) • Predefined Use Cases • Predefined Reports 2.2.2 The proposed solution alarms and searches must be unlimited functionalities and not limited functionalities, for example by the size of the deployment, such as by the number of available CPU cores.		

	2.2.3 The proposed solution must employ advanced intelligence analytics. 2.2.4 The proposed solution must perform advanced analytics against all log data or a subset of the data. 2.2.5 The proposed solution must have a risk based priority engine that can assign a risk value for all the logs, events and alarms natively at no additional cost 2.2.6 The proposed solution must automatically determine threats based on suspicious patterns of behavior. 2.2.7 The proposed solution must have the ability to automatically create whitelists of observed behavior (i.e. without manual intervention) 2.2.8 The proposed solution must have the ability to automatically learn behavioral or statistical baselines. 2.2.9 The proposed solution must offer the U.E.B.A natively out of the box. 2.2.10 The proposed solution must have the ability to leverage correlated or anomaly events back into other correlation or advanced analytics rules. 2.2.11 The proposed solution must incorporate data from multiple threat intelligence feeds into its’ advanced analytics. 2.2.12 The proposed solution must provide updated analytics rules on a regular basis to detect new and emerging threats. 2.2.13 The proposed solution must allow the organization to build a filter and reuse it with multiple of correlation rules 2.2.14 The solution must support many different types of correlation and analytics methods:		

	- Log: - Log Observed based correlation. - Non-Observed Compound based correlation. - Non-Observed Scheduled based correlation. - Session sequence based correlation. - Threshold: - Threshold observed based correlation. - Threshold non-observed compound based correlation. - Threshold non-observed scheduled based correlation. - Unique Value: - Unique value observed based correlation. - Unique value non-observed compound based correlation. - Unique values non-observed scheduled based correlation - Behavioral: - Whitelist based correlation. - Blacklist based correlation. - Machine analytics based correlation. - Statistical based correlation. - Trend based correlation **2.3 Event Response and Alerting** 2.3.1 The proposed solution must provide an ability to interface with a third-party incident response management system (e.g. Remedy, etc.)		

2.3.2 The proposed solution must provide out-of-the-box alarms designed to enforce continuous compliance and security best practices

2.3.3 The proposed solution must provide the ability to create customized alarms, distributed to specific groups of individuals and prioritize alarms and alarm delivery.

2.3.4 The proposed solution must email alarm notifications include risk rating priority level. With configurable alarm email subject line.

3 UEBA

- The UEBA must be offered Fully Integrated within the proposed solution.
- The UEBA shouldn’t be limited to the number of users.
- The UEBA must be able to detect and respond to insider threats, compromised account, and privileged account abuse
- The UEBA must collect machine data from across your environment and fill in your forensic gaps with endpoint and network monitoring
- The UEBA must correlate log information to single identities to know the actors behind the actions impacting your environment with Identity Inference, which attributes identities to anonymous log messages, streamlining forensic investigations
- The UEBA must Detect threats of data exfiltration, privileged identity misuse and fraud
- The proposed solution must share the list of predefined out of the box use cases related to UEBA

•The platform must have a list of use cases out-of-the-box and should have the ability to customize or build from scratch. Please explain how many out-of-the-box use cases are supported by the solution.

Host Forensics

The proposed solution should have an optional agent that can achieve the following:

- File Integrity Monitoring
- Process activity monitoring
- Network Communication Monitoring
- Registry keys Integrity Monitoring
- Data loss defender
- User Activity Monitoring

Administration

Ease of Use

9.1.1 Describe support for centralized administration in a geographically dispersed deployment.

9.1.2 The solution should provide centralized health monitoring of itself.

9.1.3 There must be wizards available to guide administrators through any of the administration processes.

Reporting

10.1.1 The proposed solution must offer all the reports out of the box at no additional cost.

10.1.2 The solution must include pre-defined reports.

10.1.3 Reports must be scheduled and delivered to the recipients in an automated manner. Reports must be restricted to different levels of management within the company.

<table>
<tr><td></td><td>It must have a rest API to allow 3rd party tool to query and report the logs such as Kibana for instance.</td><td></td><td></td></tr>
<tr><td><b>1xRack based server 19" (2U)</b></td><td>
<table>
<tr><td><b>CPU</b></td><td>2xIntel® Xeon® Gold 5317 (12C, 3.0 GHz, TLC: 18 MB, Turbo: 3.40 GHz, 11.2 GT/s,</td></tr>
<tr><td><b>Memory</b></td><td>8x32GB (1x32GB) 2Rx4 DDR4-3200 R ECC</td></tr>
<tr><td rowspan="2"><b>Disk</b></td><td>16xHD SAS 12G 1.2TB 10K 512n HOT PL 2.5' EP</td></tr>
<tr><td>4xSSD SATA 6Gbs 480 GB</td></tr>
<tr><td><b>Raid Controller</b></td><td>1xPRAID EP680i LP
SAS/SATA/PCIE-NVMe RAID Controller based on LSI Mega RAID SAS3916
- for up to 16 internal SAS/SATA HDD, SSD, for mixed configuration SAS, SATA and up to 2 times x4 PCIe-NVMe SSD
- RAID Levels 0, 1, 10, 5, 50, 6, 60
- TFM already included
- 8GB Cache
- Safe Store and Fast Path included
- Cache Cade® not any longer supported</td></tr>
<tr><td><b>Lan</b></td><td><b>Lan 1</b>: 2x10GBASE-T PCIE LP
<b>Lan 2</b>: 4x1Gbit</td></tr>
<tr><td><b>PSU</b></td><td>2x900W modular Power Supply Module ,</td></tr>
<tr><td><b>Rack Mount Kit</b></td><td>2xRack Mount Kit (RMK) for server max.</td></tr>
<tr><td><b>Power Cord</b></td><td>2xCable power cord rack, 1.8m, black Power cord for rack mounting+, IEC 320 C14 -> C13 (10A plug), 1.8m</td></tr>
<tr><td><b>System Management</b></td><td>iRMC advanced pack (Remote Graphical Console)</td></tr>
<tr><td><b>Warranty</b></td><td>Standard Warranty 3years</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td><b>Training</b></td><td>Professional level class room and hands on training by principal only.</td><td></td><td></td></tr>
</table>

Requirements	Details	Yes	No
	1. Proposed SIEM software and hardware must be in Leaders of Magic Quadrant of Gartner of July, 2021. 2. The proposed hardware market launch date should not be before 2020. Also provide the product roadmap for next 5 years (2022 onwards). 3. Installation and configurations with respect to NRSP Network design and NRSP Business requirements. 4. The supplier should provide a plan for Support, Warranty and Services in its technical proposal. 5. 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. 6. Only brand new hardware to be proposed. Refurbished, Grey or smuggled or international warranty products will be not accepted in any case. 7. Presentation of proposed hardware at NRSP premises to the technical/user team.		

DELIVERY TIME: ______________________

BREIF WORK PLAN:

Authorized Signature: ______________________

Stamp: __________________________________

Date: ___________________________________

Form F1

(To be submitted on firm/company letter head)

FINANCIAL PROPOSAL SUBMISSION FORM

[Location, 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 Tender No. NRSP/SIEM Software and Server Hardware EQUIPMENT /RQ-677

Sir,

We, the undersigned, offer to provide the equipment & services to NRSP, in accordance with your subject tender. 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 Cell No.:

Form F2

(To be submitted on firm/company letter head)

FINANCIAL PROPOSAL

S. No.	**Description**	**Make/Model/Version**	**Qty**	**Unit Price**	**GST**	**Total Price with GST**
1	NGN SIEM Software		1 Each			
2	Rack based server 19" (2U)		1 Each			
3	Professional level class room and hands on training by principal only.		2 Persons			
4	Installation, testing, configuration (if any)		1 Job			
Grand Total: (Including all charge and taxes)						

Validity:

Delivery Time:

Any other details or terms & conditions:-

Authorized Signature: ________________________
Stamp: ______________________________________
Date: _______________________________________

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.

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.