PRE – BID MEETING MINUTES

Procurement of Security Information & Event Management Solution (SIEM) and Allied Services for NatCat Data Centers of NDRMF

File No.:	IFB NO. 004/36/IT
IFB Published Date:	17th January 2025 – PPRA EPADS and NDRMF Website, 21st January 2025 – Print Media and PPRA Website – TS555313E
Bids Submission Date & Time:	06th February 2025 @ 1100 Hours via PPRA EPADS
Pre-Bid Meeting Date & Time:	28th January 2025 @ 1100 Hours
Pre-Bid Meeting Venue:	NDRMF Board Room, 5th Floor EOBI House G-10/4 Islamabad

1. NDRMF's Representations:

1	Manager (Procurement)	2	Deputy Manager (IT)
3	Deputy Manager (MIS)	4	AM (Procurement)

2. Bidders' Representations:

Four (4x) Bidders six (06) representatives participated in the subject Pre-Bid Meeting

3. Proceeding of Meeting:

The Pre-Bid Meeting started with brief introduction and tender specific information. Bidders have actively participated in the meeting and shared several queries related to tender responses preparation & terms in general and special conditions of contract, and Section V: Scope of Work. All general queries were responded while technical queries were discussed and conveyed to bidders that a refined response with detailed clarification will be shared in the form of meeting minutes. Henceforth, NDRMF response in form of pre-bid meeting minutes are divided into following two sections;

Section 1: Queries related to Tender Preparation and Term & Conditions - General
Section 2: Queries related to Scope of Work - Technical

Section 1: - Tender Preparation and Terms & Conditions - General:

No.	Bidder Clarification Queries	Bidding Doc. Reference	NDRMF Response
1	Should there be separately financial and technical Bids?	Section I Clause 4	Bidding shall be conducted in line with the Single Stage One Envelope procedure of the Public Procurement Rules 2004, and E-PADS Regulation 2023 wherein you are required to prepare both Financial and Technical proposal/credentials, duly signed and stamped by authorized officials; which shall be scanned in good readable in a single PDF file and uploaded on PPRA EPADS (www.eprocure.gov.pk) while original Form – 5 of Bid Securing Declaration shall be submitted in IFB Notice stated Address.
2	Required submission of document for evaluation of eligibility and qualification.	ITB No.11.1 r/w BDS No.11	The tender document (TD) has clearly indicated in BDS No.11 and BDS No.17 (Page No.33/72 of TD) the required documents to be submitted for evaluation of eligibility and qualification. Apropos above, bidders must submit duly filled, signed and stamped all responses schedules clearly indicated at 41/72 of TD while special attentions shall be given to Technical Compliance Sheet at (Section VI Form 3.2 on page 45-47/72), Form 4.1 and 4.2. while incorporating 90 days Logs retention resources requirements.

No.	Bidder Clarification Queries	Bidding Doc. Reference	NDRMF Response
3	Status of Earnest Money/Bid Security as stated in instruction to bidders?	ITB No.18 r/w BDS No.22	Bidders were informed that PPRA in its bidding template has indicated detailed instructions to Bidders in Section No. II (Page No.5 – 31/72 of subject tender) which are generalized information however it is supplemented by Section No. III i.e. BDS - Bidding Data Sheet (Page 32 – 35/72 of subject tender). Hence the bidder(s) shall always refer to BDS. As per BDS No.22 at page#34/72, Bid Security Declaration is required **as per Form 5;** respective Form is provided on page 49/72.
4	Can a bidder submit alternative Bid.	ITB No.19.1 r/w BDS No.23	Alternative Bids are not allowed under subject tender.
5	Bidder's Authorization	ITB No.21.2 r/w BDS No.25	Corresponding instructions are clearly indicated in BDS No.25 at page#34/72 of tender document. With respect bidders' clarification regarding MAL – Manufacturer Authorization Letter; **it was clarified that the said MAL for SIEM Solution submission along with Bid is mandatory.**
6	Performance Guarantee status?	ITB No.43.1 r/w BDS No.28	The Performance Security (or guarantee) shall be five (05%) percent of contract value either in form of Bank Guarantee (Form attached in tender doc) or Bank Draft/CDR/SDR, which shall be discharged following completion of post certification support or expiration of contract, or whichever is earlier.
7	Payment Terms	SCC Clause 18 r/w GCC 41.1	The tender document (TD) has clearly indicated milestone-based payment terms in SCC Clause 18 r/w GCC 41.1 (Page 67/72 of TD). No deviation in payment terms will be allowed.

Section 2: - Queries related to Scope of Work - Technical

No	Referred Section of Bidding Document		Bidder Clarification Queries	NDRMF Response
1		Section V: Scope of Work	Will the bidder have to procure hardware or will be provided by NDRMF?	Hardware will be provided by NDRMF.
2		-do-	Can we Quote Licensing Model based on log volume or EPS (events per second)?	No, licensing model must be based on number of devices.
3		-do-	List of equipment available at Data Center Setup, Device integration, bandwidth etc.	Certain related information is provided in Section V: Scope of Work of the tender document while the list of Devices/Applications is enclosed at **Annex-A** to these minutes.
4		-do-	Clarification in Section V: Scope of Work; Clause 3 (b) 2 post deployment support.	Said Clause 3, b, 2 of Section V of tender document, shall not be read as a part of post deployment rather this clause is applicable for implementation phase. Post deployment support will be 24/7 remotely with physical visits when needed.

No	Referred Section of Bidding Document		Bidder Clarification Queries	NDRMF Response
5		-do-	Please find attached the log sources inventory sheet, please fill it with all devices that will be integrated with SIEM.	Please refer to **Annex-A** enclosed herewith encompassing devices and applications.
6		-do-	What is the bandwidth and the type of connectivity between each site and which site the SIEM will be hosted?	SIEM will be deployed at PR site. MPLS point-to-point link with 20 Mbps bandwidth.
7		-do-	What is the online (uncompressed) retention period in months required for the logs?	90 days (3 months)
8		-do-	What is the offline (compressed) retention period in months required for the logs?	90 days (3 months)
9		-do-	What are the number of users on each site?	Please refer to **Annex-A** enclosed herewith encompassing devices and applications.
10		-do-	Are there specific use-cases that you are interested in deploying on SIEM? Please list them.	Clearly mentioned in Section V: Scope of Work e.g. Correlation, Vulnerability assessment, FIM, ISO 27001 mapping etc.
11		-do-	Is DR setup required?	No.
12		-do-	Are you looking for hardware options from Fortinet or virtual machines will be provided?	NDRMF will provide the virtual machine
13		-do-	If Hardware is required, can you provide the collector virtual machines? Collectors are a lightweight machine that are used to receive the logs and forward it to SIEM core components.	Agents will be deployed on endpoints and network logs will be collected from Syslogs.
14		-do-	Are there business applications or custom apps required to be integrated with SIEM? If yes, how many are there and please included it in the log sources sizing sheet	Please refer to **Annex-A** enclosed herewith encompassing devices and applications.
15		-do-	The license type required is subscription or perpetual?	Annual Subscription
16		-do-	The license term is 1 or 3 or 5 years?	One Year
17		-do-	Is HA setup required?	No.
18	1.5. b	Real-time Threat Detection: Proactively identifying and alerting suspicious activities and cyber threats	Proactive defense requires deployment of minimum 3 x systems including SIEM, NDR and EDR. Proactive / Real time detection cannot be performed through deployment of just SIEM and/ or EDR (since EDR is already deployed). Kindly elaborate requirement that whether deployment of NDR is required or else. It has to be kept in mind that EDR can be bypassed by APTs but evasion of NDR is not possible	Only SIEM will be required for Real-Time Threat Detection as it will collect, correlate and identify the attackers from the devices connected with it.
19	1.5. c	SOAR responses and playbook	The point should be discussed in detail. As playbooks and responses are part of SOAR not SIEM	We are not looking for Separate SOAR application but to have a response functionality within SIEM and such functionalities are offered in top SIEM application
20	1.5. d	Ensuring compliance with relevant industry regulations and maintaining	Please specify that compliance and auditing of only end point systems/ servers is required or compliance and auditing of Network appliance (routers, switches, firewalls etc.) is also required	Compliance mapping is required for endpoints and servers only.

No	Referred Section of Bidding Document		Bidder Clarification Queries	NDRMF Response
		comprehensive audit trails		
21	3.a.2	Raw Logs for Advance Searching	Raw log archiving requires deployment of Data Lake. Which increases the cost. Please specify if this requirement is mandatory	Raw logs module must be part of SIEM application as this will be required for Threat Hunting, Separate data lake solution is not required.
22	3.a.11	Auto Asset Discovery for identification of Unknown Devices	This requires the deployment of NDR. Or any other network monitoring system. Please specify whether network monitoring/ NDR system is required or not.	Auto Asset Discovery module needs to be part of SIEM application to identify the unknown devices in SIEM
23	3.a.12	automated, manual and time-based backup to fulfil the continuity of business/ operation as well as integrity.	This point should be discussed as the SIEM is a security control for incident detection and backup for BCP/ DRP.	Backup functionality needs to be part of SIEM application
24	3.a.13	Compliances Module (NIST, HIPAA, PCI DSS, GDPR, IOS, SOC 2, ADSIC, CIS and NESA)	Compliance is only required for endpoints/ servers/ workstations or also for network devices	Compliance mapping is required for endpoints and servers only
25	3.a.28	USB Detection Logs in the Network	USB detection logs can only be fetched from endpoints and not from Networks. Please explain	Yes, these logs will be captured from endpoints
26	3.a 30	SNMP Traps and Device NetFlow	Will it be based on NDRMF device, monitor network traffic and provide net flows or it should be vendor/ bidder device. If network monitoring means NDR functionality then it should be discussed.	SIEM must have the capability to ingest SNMP Traps and NetFlow. No other application is required.
27	3.a.35	Organization Risk Score or Security Posture or Internal Attack Surface Management dashboards	Please specify that Sangfor EDR has to be integrated, or system logs has to be fetched separately for integration with SIEM	EDR Logs will be fetched from EDR Server
28	3.a.37	Configure Email Alerts with Severity Level	Please explain, does it mean deployment of an email security system?	Email Alerting needs to be part of SIEM application.
29	3.a.72	Assigning IOCs to User	This point is not clear. Please elaborate	IOC must be associated with some Device.
30	3.a.78	SIEM must collect and process logs from various sources, including routers, switches, servers, firewalls, IDS/IPS, applications, databases, and endpoints.	Does it mean separate log collection from systems. Can Sangfor EDR logs be ingested in SIEM for this purpose?	Logs will be directed fetched from all devices. EDR will be one log source
31	3. f	The cost is based on per device.	Based on their nature/ features/ functionality, some of the devices may generate less number of events other may be large. The estimation of storage for	Cost is based on one device. Estimated events per second (EPS) will be 7,500

No	Referred Section of Bidding Document		Bidder Clarification Queries	NDRMF Response
			retention of raw/ processed logs/ events is difficult.	
32	NA	100 Device License	Please elaborate as most commercial SIEM solutions are sized based on Events/sec. Also please elaborate out of 100 Devices how many are servers, Desktops/Laptops, Network Elements.	EPS will be around 7,500

NOTE:

a) Bidders' sought clarification information asked through email(s) are also incorporated in these meetings for general information of all prospective bidders. These Pre-Bid Meeting minutes shall be construed as a mandatory part of the bidding document. These meeting minutes supplements subject issued bidding document and where (if any) mentioned supersedes respective clause(s)/section(s)/information(s) of the said issued bidding document.
b) Financial impact in line with subject bidding document and these minutes must be incorporated by bidders accordingly.
c) The timeline will remain the same, hence shall be strictly followed by bidder. Extension in Bid submission will not be made.

ANNEX - A

Devices/Applications for SIEM Solution			
S. No	**OS**	**Total**	**Model**
1	Linux	10	Ubuntu, SUSE Enterprise for SAP
2	Windows	15	Windows Server 2022, Windows 11
3	VMWare	7	Vcenter, SRM, Vrealize Ops
4	Switches	14	Cisco N9K-C93180YC-FX, Cisco C9200L-24P-4X-E
5	Routers	3	Cisco C8300-1N1S-42TX
6	Wireless Controllers with Access Points	12	Cisco C9800-L-F-K9, Cisco C9105AXI-G
7	Firewalls	3	Sangfor NGAF M5400-F-I
8	Internet Access Gateway (IAG)	1	Sangfor IAG M5100-AC-I-S
9	Secure Manager (EDR)	1	Sangfor Endpoint Secure with Secure Manager
10	Physical Servers	6	Dell VX-Rail VP-760
11	Virtual Tape Library (VTL)	1	Dell Power Protect DD6400
12	Backup Software	1	Dell Power Protect
13	MS Office 365	1	
14	End users	20	
15	Customize Application Servers	5	SAP ERP, NatCat, Career Portal,
	Total	**100**	