Corrigendum - 3

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for "SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL."

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
1	(2.01) Technical Criteria (5)	6	Bidder must have at least 3 deployments for 20000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period ending bid submission date) for proposed SIEM solution.	This clause is restricting multiple OEMs of different make and models to participate in the tender because in each and every bid or tender,the products quoted regularly will change and the bidder always looks at the best commercial models quoted by the OEM. So it will be difficult for OEMs as well as bidders to participate in this opportunity. Kindly requesting to Amend or Modify the Clause as " Bidder must have at least 3 deployments for 20,000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period ending bid submission date) for proposed / Similar SIEM solution ".In case the bidder does not have such experience, the Installation, commissioning, integration, tuning of tools shall be in OEM scope. An undertaking from OEMs along-with proposed scope of work shall be submitted.	No Change in the RFP clause
2	Technical Specification	16	116) Customized Reports: The proposed solution must provide the ability for customers to create their own reports with report templates, reporting wizard as well as an advanced interface for power users to create their own custom report queries.	This feature is specific to the capabilities of certain OEMs, Kindly requesting you to amend /modify the clause as "Customized Reports: The proposed solution must provide the ability for customers to create their own reports with report templates and reporting wizard."	**Amended Clause:** Customized Reports: The proposed solution must provide the ability for customers to create their own reports with report templates and reporting wizard
3	SCOPE OF WORK	105	The proposed solution built-in FIM (File Integrity Monitoring) must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data	Kindly requesting to amend this clause as " The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data".	**Amended Clause:** The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data
4	Network Detection and Response (NDR) Specifications: (Page -99)	99	By collecting, analyzing and storing information from various sources, the NDR System should provide a full audit trail of all network transactions and perform more effective forensic investigations.	**Clarification -** Various sources means here, Variour network vantage points for traffic capture. Please clarify	Various sources means variuos network points for traffic capture
5	Network Detection and Response (NDR) Specifications: (Page -100)	100	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	**Requested Change -** The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL or packet capture based solution. **Justification-** It is contradicting with clase 1.3, It says, The proposed solution must support full packet capture and smart capture. Here clause is talking about flow based system. Packet capture based system have all the visibility while flows have limited informations. Hence request to change the clause as requested.	**Amended Clause:** The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL or packet capture based solution.

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
6	Network Detection and Response (NDR) Specifications: (Page -100)	100	The solution should be able to combine the flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation.	**Requested Change -** The solution should be able to combine the packet/flow records coming from different traffic capture vantage for example network devices like routers, switches, firewalls thatare associated with a single conversation. **Justification-** It is contradicting with clase 1.3, It says, The proposed solution must support full packet capture and smart capture. Here clause is talking about flow based system. Packet capture based system have all the visibility while flows have limited informations. Hence request to change the clause as requested.	**Amended Clause:** The solution should be able to combine the packet/flow records coming from different traffic capture vantage for example network devices like routers, switches, firewalls thatare associated with a single conversation.
7	Network Detection and Response (NDR) Specifications: (Page -100)	100	The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.	**Requested Change -** The solution must be able to stitch packets/flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address. **Justification -** This is packet based functionaity to stich the conversation before and after Nating using X-forwarder in the packet. Hence request to change the clause as requested.	**Amended Clause:** The solution must be able to stitch packets/ flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.
8	Network Detection and Response (NDR) Specifications: (Page -101)	101	Ability to detect ransomwares and profiling malwares such as Troldesh, Dridex, Quakbot, TrickBot, Gootkit, Adware, TorrentLocker, Adwind,Tofsee, Gozi, Jbifrost, Dyre, ZeuS Gameover, chinAd, bamital, Post Tovar GOZ, corebot, cryptominers, etc	**Requested Change -** Solution should be able to detect and monitor ransomwares and malwares. **Justifications -** There are thousands of Malware and various ransomware attacks in the world. Keeping only these names is bit certain OEM specific. Hence request to change the clause as requested.	**Amended Clause:** Solution should be able to detect and monitor ransomwares and malwares.
9	Network Detection and Response (NDR) Specifications: (Page -102)	102	The solution should detect events of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including network flood events of ICMP, UDP, TCP SYN, TCP NULL, IP NULL, identify the presence of botnets in the network, etc. and detect long-lived connections that may be associated with data-exfiltration.	**Requested Change -** The solution should detect events of denial-of-service (DoS) with IoCs/Behavioural (deviation from normal routine traffic) and distributed denialof-service (DDoS) attacks with using IOCs/ Behavioural (deviation from normal routine traffic) including various network flood events and identify the presence of botnets in the network etc. and detect long-lived connections that may be associated with data-exfiltration. **Justification -** Clase talks about only few specific DDoS attacks without detection methods. Hence request to change the clause as requested.	**Amended Clause:** The solution should detect events of denial-of-service (DoS) with IoCs/ Behavioural (deviation from normal routine traffic) and distributed denialof-service (DDoS) attacks with using IOCs/ Behavioural (deviation from normal routine traffic) including various network flood events and identify the presence of botnets in the network etc. and detect long-lived connections that may be associated with data-exfiltration.
10	SOAR Specification : Reporting		Solution should provide integrated BI platform to help create advanced Dashboards and reports based on KPI's to be tracked	Requets for amending the clause as "Solution should provide integrated BI platform or other customization options to help create advanced Dashboards and reports based on KPI's to be tracked."	**Amended Caluse:** Solution should provide integrated BI platform or other customization options to help create advanced Dashboards and reports based on KPI's to be tracked.
11	Delivery Schedule		Delivery/completion within 06 months from the LOI/PO date.	Delivery/completion within 08 months from the PO date.	No Change in the RFP clause
12	17.0 One Bid Per Bidder:Pt 17.01		Each Bidder shall submit only one Bid by itself. No Joint venture is acceptable. A Bidder who submits or participates in more than one Bid will cause all those Bids to be rejected.	We understand this is applicable for bidders/system integrators. I.e. While one bidder can put only one bid, but different bidders can put same OEM stack bid. Kindly confirm.	Yes, understanding is correct

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for "SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL."

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
13	QUANTITY AND DELIVERY REQUIREMENTS: Part A & Part C			In both Part A & Part C; for line item 1 to 4, there is no mention of so of support/warranty year. Kindly confirm, whether SW & HW support warranty needs to be factored for 1 year or 3 year ?	Please refer warrant/support section for more detail
14	PRICE BID FORMAT FOR BRPL & BYPL: Part A & Part C			In both Part A & Part C; for line item 1 to 4, there is no mention of so of support/warranty year. Kindly confirm, whether SW & HW support warranty needs to be factored for 1 year or 3 year ?	Please refer warrant/support section for more detail
15	UEBA (User Entity and Behavior Analytics) Specification: Pt 6		The agents of the solution should not be open sources, the agents should be from the same OEM and should not contain any malicious code. OEM to provide declaration for the same.	When it comes to UEBA, most of the OEMs work upon agentless approach. Agent based approach is mainly used by EDR/XDR solution who does not have a dedicated UEBA offering. However in our case our solution is completely agentless and does not need any agent to perform the task. Kindly allow agentless solution as well.	**Amended Clause:** The agents of the solution should not be open sources, the agents should be from the same OEM and should not contain any malicious code. OEM to provide declaration for the same. OEM can also suggest agenless approach/solution.
16	UEBA (User Entity and Behavior Analytics) Specification: Pt 15		Use of supervised machine / deep learning algorithms	Different OEMs use different methodology to detect anomalies. We perform the same via applying AI and machine learning capabilities like advanced data mining, graph theory, statistical, predictive analytics etc. Hope this is inline to your requirement. Kindly confirm.	**Amended Clause:** Use of supervised machine / deep learning algorithms or other diferent methodology to detect anomolies
17	UEBA (User Entity and Behavior Analytics) Specification: Pt 19		The solution should be an endpoint based UEBA, where the UEBA will take inputs from endpoint protection devices to further detect anomalies	When it comes to UEBA, most of the OEMs work upon agentless approach. Agent based approach is mainly used by EDR/XDR solution who does not have a dedicated UEBA offering and need inputs from endpoint based solution. However in our case our solution is completely agentless and does not need any agent to perform the task. Kindly allow agentless solution as well.	**Amended Clause:** The solution should be an endpoint based UEBA, where the UEBA will take inputs from endpoint protection devices to further detect anomalies. OEM can also suggest agenless approach/solution.
18	UEBA (User Entity and Behavior Analytics) Specification: Pt 24		The proposed solution must have built in File Integrity Monitoring, Process activity monitoring, Registry Integrity Monitoring with no additional cost	Features asked against this point like FIM are not part of UEBA solution. This seems specific to any OEM, request you to kindly delete this clause.	**Amended Clause:** The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data
19	UEBA (User Entity and Behavior Analytics) Specification: Pt 52		Use of supervised machine learning algorithms	Different OEMs use different methodology to detect anomalies. We perform the same via applying AI and machine learning capabilities like advanced data mining, graph theory, statistical, predictive analytics etc. Hope this is inline to your requirement. Kindly confirm.	**Amended Clause:** Use of supervised machine learning algorithms or any other methodology to detect anomalies.
20	SCOPE OF WORK: Pt. 1.14		The Platform must include log management, NG SIEM, Host Forensics, UEBA, NDR, File Integrity Monitoring, Security Analytics, Big Data 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)	Host forensics and FIM solution is not part of SIEM technology. Reqeust BSES to remove the host forensics and FIM requirement.	**Amended Clause:** The Platform must include log management, NG SIEM, UEBA, NDR, Security Analytics, Big Data Analytics, Security Automation and Orchestration engine (includes but not limited to Incident Management, Incident Response), Advanced Correlation within the same platform or mix of platforms with closed intergration between all modules.

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
21	SCOPE OF WORK: Pt. 1.18		The proposed solution built-in FIM (File Integrity Monitoring) must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data	FIM solution is not part of SIEM technology. Reqeust BSES to remove the FIM requirement.	**Amended Clause:** The proposed solution should integrate with FIM (File Integrity Monitoring) and must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data
22	2.01 (4)	6	Can we add that a bidder should have atleast 1 SOC client in power sector	This would help in bringing in the bidder's expertise of threat management of power sector	No Change in the RFP clause
23	2.01 (4)	6		Disclosing the client name and contact details may not be disclosed as per the NDA signed with respective clients	Tender Condition shall prevail.
24	29	18	PBG for 60 months while the contract is for 3 years operation; PBG should be for 36 months	The contract is structured for 3 years of operations theerafter it is only the warranty period. Recommend the ask of PBG for two phases accordingly.	Warranty shall be 5 years & it shall supersede warranty clauses stated elsewhere in the NIT. PBG to be submitted for Warranty period
25	Annexure 1.06	26	Request to remove the annexure as this may not be applicable		Tender Condition shall prevail.
26	Annexure 1.09	28	Some of the details like Customer Name, PO Number, etc may not be disclosed as per the NDA signed with respective clients		Tender Condition shall prevail.
27	Annexure 1.12 and 1.13	31	May not be required		Please mention Not applicable and submit bid.
28	Quantity and Delivery Requirements	59	Please provide baseline for NDR solution in terms of Flow per minute	The same is required from a sizing and licensing perspective	Baseline needs to be done as per quatam provided in the RFP.
29	Price Bid format	69	The understanding is that the break up price for incremental 1000 EPS has to be provided for any requirement over and above 10000 EPS.		Yes, understanding is correct
30	Technical Specifications - 1	73	Does the solution need to support OT protocol as well	This would enable to identify the appropriate solution to support.	Yes, understanding is correct
31	Technical Specifications - 59	78	Support for operational technology (OT) and Internet of Things (IoT) technologies and environments (e.g., ICS/SCADA).	Please confirm the existing OT solution	All avaliable OT solutions in industry like Claroty, Nozomi, Opswat, Tenable, etc.
32	2.1	108	BRPL & BYPL will provide the access of security devices like WAF, SIEM and SOAR etc installed at BRPL & BYPL premise and bidder needs to monitor and manage its operations.	WAF would be integrated with SIEM and relevant alerts would eb monitored on SIEM console.	Yes, understanding is correct
33	2.1 (m)	108	Bidder should be MSSP having SOC 2, Type II certified. Certified report – 1st page of report to be submitted	The solution and operations is being delivered from BSES premises. The bidder's infra/ premises will not be utilised. Therefore, the requirement for the certification may not exist.	**Ameanded Clause:** Bidder should be MSSP having SOC 2, Type II certified. Certified report – 1st page of report to be submitted (OPTIONAL)
34			Penalty amount to be limited to 5% of the quarterly amount		Tender Condition shall prevail.
35		114	Quality of Resource and Availability - There should not be any penalty on this criteria as the other SLA parameters indirectly covers the quality of resources		No Change in the RFP clause
36	7	73	High-Level Diagram to be submitted for SoC solution ensuring no data loss and optimal bandwidth utilization in WAN and LAN.	This should be part of deliverables of the successful bidder as it may not be able to envisage BSES network at this stage.	This should be submitted along with technical bid document.

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
37	17		The solution shall allow bandwidth management, rate limiting, at the log collector level.	This is usually a network operations functionality. Kindly clarify.	Yes, understanding is correct
38		60	The EPS burst should be processed in real time without dropping or queuing to ensure real time analysis of threat.	This would need periodic eps baselining to ensure licensing is meeting the average count	Ok
39	20	96	The solution should be installed passively into infrastructure	The deployment tools to be provided by BSES. Kindly confirm	Passively means solution to be deploy without distrubing running infrastructure.
40	1.21	106	The next gen SIEM solution should support high availability features and should be proposed in HA mode for all layers at DC	Should hardware be sized for HA. Kindly confirm	Yes, Hardware to be plan in HA
41	1.39		Custom parser development required during implementation and operations phase will be in bidder’s scope.	A finite scope in terms of parsers can be helpful in scoping	No Change in the RFP clause
42	2,1(i)	108	Bidder should evaluate BSES ticketing system to log tickets of SOC and if found existing ticketing system to be incapable then access to bidder ticketing system to be provided to BRPL & BYPL for tracking purpose and SLA calculations	Kindly provide the existing Ticketing solution at BSES.	Curent tool is Everest also a seprate RFP for ITSM is floated to finalize the ticketing tool.
43	113		High Criticality Security Alerts (Priority1) to be reported within 30 minutes and resolved within 1 hour	Resolution is in BSES scope. It cannot be resolved by the bidder as the infra is not in bidder's control.	Ok, But support is required from bidder to get the security alerts closed.
44	REQUEST FOR QUOTATION	4	Earnest Money Deposit (EMD)	Requesting to please provide MSME Exemption for EMD waiver.	Tender Condition shall prevail
45	Qualification Criteria	16	The bidder should have average turnover of Rs. 50 Crores in at least three financial years last three years (i.e. 2021-22, 2022-23, 2023-24)	We request you to please relax the clause for MSME/Start Up. Kindly give the financial exemption to them as per GOI Guideline. Also if not then kindly reduce the average turn over to 20 Cr for last 3 years	Tender Condition shall prevail
46	Qualification Criteria	16	The Bidder should be a Managed Security Service Provider (MSSP) having its own Security Operations Centre (SOC) operating since last 5 years from the date of bid submission, from where it is providing services to different customers	Please confirm this clause clearly, SI can fulfill this, or OEM also must match this QR. Hope, SI can participate with any technical qualified OEM & the same QR apply to SI not the OEM.	Bidder should have its own SoC which in operations since last 5 years.
47	Qualification Criteria	16	Bidder must have at least 3 deployments for 20000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period ending bid submission date) for proposed SIEM solution	Requesting to please allow the bidders experience on device-based count not the EPS based. Otherwise please allow for 1 deployment for 10000 EPS for maximum participation.	In case of device, bidder must have at least 3 deployments for 5000 device or one deployment for 10000 devices each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period ending bid submission date) for proposed SIEM solution. (device should have 50% servers, 25% networ/routing, 25% firewall and security devices)

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
48	Qualification Criteria		The Bidder should be a Managed Security Service Provider (MSSP) having its own Security Operations Centre (SOC) operating since last 5 years from the date of bid submission, from where it is providing services to different customers	Since the requirement is for onsite implementation of SOC, hence request to remove the requirement of MSSP to have their own SOC centre. And also consider limiting the PO requirement for on-premise implementation and services delivery for 3 clients so that more MSSP can participate in the RFP requirement.	No Change in the RFP clause
49	1.05 Time Schedule	3	The tender has been invited for both the discom i.e. BSES Yamuna Power Limited (BYPL) and BSES Rajdhan Power Limited (BRPL). All the tender process for both the discom will be carried simultaneously as per the process. After finalization of rates and agency for award, separate contracts will be awarded by both the discom. All the clauses of this NIT, which are applicable to BYPL shall also be equally applicable to BRPL	Request you to clarify if our under standing is correct, " Bidder will provide the pricing for Hardware, Software, SIEM, SOAR, NDR, UEBA etc and Resource requirement for BYPL and the Same will be part of the BRPL. And based on this BRPL will release a seperate PO accordingly" Kindly confirm the BRPL Location.	Clause is clear, Also refer price bid format. BRPL location is in Delhi.
50	19.02	10 or 50	24x7, 4 hrs resolution, 5 years onsite Warranty (part and labor), support from OEM along with all patches for hardware and softw	Request BYPL to amend the clause as "24x7, **4 hrs response**, 5 years onsite Warranty (part and labor), support from OEM along with all patches for hardware and software" The resolution is on the best effort basis.	No change in the RFP clause
51	1.4	Page 31 of 36	The solution should be sized for 2 Gbps from day one with ability to scale upto 10 Gbps in future.	The solution should be sized for 2 Gbps from day one with ability to scale upto 5 Gbps in future without any hardware augmentation and to 10Gbps and beyond through hardware augmentation. Reason: 2 Gbps to 5 Gbps is 150% growth, factoring for higher hardware from day 1 is wasting of resources.	No change in the RFP clause
52	3.2	Page 32 of 36	Network Detection and Response (NDR) solutions leverage the inherent flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.	Network Detection and Response (NDR) solutions should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes. **Justification:** This has a dependency on the network equipment to generate flow. Also, almost all NDR solutions are based on throughput and not on FPS, Full packet based NDR offers much more value than FPS based solutions as FPS is good for only network performance monitoring and not apt for security monitoring. Infact top 5 leaders of NDR are all full packet capture/throughput based.	**Amended Clause:** Network Detection and Response (NDR) solutions leverage the inherent packet/ flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics, represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.
53	3.4	Page 32 of 36	NDR solution should be able to use the existing network environment as a sensor grid to analyze traffic flow across the across the existing network and security solutions in a nondisruptive manner	NDR solution should be able to use the existing network environment to analyze traffic across the across the existing network and security solutions in a nondisruptive manner. **Justification:** Removing the dependency on the network for using it as a sensor grid.	**Amended Clause:** NDR solution should be able to use the existing network environment to analyze traffic across the across the existing network and security solutions in a nondisruptive manner.

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
54	3.10	Page 33 of 36	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	Solution should ensure lossless packet and payload capture upto 2 Gbps sustained performance from day one with ability to scale upto 5 Gbps in future without any hardware augmentation for complete protocol analysis. **Justification:** This clause is OEM-specific. NetFlow and NSEL is a Cisco proprietary protocol.Cisco Network Security Event Logging (NSEL) is a proprietary Cisco protocol (https://www.google.com/search?q=cisco+nsel+proprietary+&sca_esv=35aa2c76c27153e3&rlz=1C1RXQR_enIN1099IN1099&sxsrf=ADLYWIL3bNukpUaiKAuqUsqn20A8kl8ZGQ%3A1734517258279&ei=CqJiZ9yyEOe84-EPmtDzuAw&ved=0ahUKEwjc36SojLGKAxVn3jgGHRroHMcQ4dUDCBA&uact=5&oq=cisco+nsel+proprietary+&gs_lp=Egxnd3Mtd2l6LXNlcnAiF2Npc2NvIG5zZWwgcHJvcHJpZXRhcnkgMgUQIRigATIFECEYoAEyBRAhGKABSJlIUOwBWJpGcAF4AZABAJgBqAOgAfosqgEIMi00LjExLjK4AQPIAQD4AQGYAgygAtEdwgIKEAAYsAMY1gQYR8ICBhAAGBYYHsICCxAAGIAEGIYDGIoFwgIIEAAYgAQYogTCAgcQIRigARgKwgIEECEYFZgDAIgGAZAGBJIHCTEuMC4yLjcuMqAHnzw&sclient=gws-wiz-serp)	Read the clause clarefully we are not limiting only to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL. We are not limitting on flow type and allowing all forms of flows. No change in the clause
55	3.11	Page 33 of 36	The solution should be able to combine the flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation	To be deleted. **Justification:** Not required as most NDR looks at full packet and do not need to stitch flows as this is a limitation of flow based NDR solutions	**Amended Clause:** The solution should be able to combine the packet / flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation
56	3.12	Page 33 of 36	The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.	To be deleted. **Justification:** Not required as most NDR looks at full packet and do not need to stitch flows as this is a limitation of flow based NDR solutions	**Amemded Clause:** The solution must be able to stitch packets/ flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.
57	5.5	Page 36 of 36	The solution should integrate with OpenLDAP, Microsoft Active Directory, RADIUS and DHCP to provide user Identity information in addition to IP address information throughout the system	The solution should provide full historical mapping of User Name to IP address logins in a searchable format without any dependency on the network **Justification:** Let us suggest what needs to be done rather how it should be done which is OEM specific	Yes, Understanding is correct
58	STATUTORY & CYBER SECURITY COMPLIANCE		To comply with the requirement of the Ministry of Power, the Bidder has to provide artifacts/certificates against the below points along with or before delivery of material/invoice. • All software components are tested in the country, to check for any kind of embedded malware/Trojan/cyber threat and for adherence to Indian Standards. i. All such testing has been done in certified laboratories designated by the Ministry of Power (MoP).	Request to delet this point, or clarify on designated by the Ministry of Power	No Change in the RFP clause. Clause is self explanatory
59	VOLUME – III TECHNICAL SPECIFICATIONS	73	SoC solution must be dedicated on premise solution and support IT and OT	Which kind of OT devices need to be integrated with SOC solution?	OT solutions in industry like (but not limited to) Claroty, Nozomi, Opswat, Tenable, etc

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
60	VOLUME – III TECHNICAL SPECIFICATIONS	96	Proposed NDR Systems should be hardware-based appliances.	All components SIEM,SOAR, NDR, UEBA required from single OEM?	Can be from single OEM and can be from different OEM. In case of different OEM tight intergatrion needs to be ensure by the bidder.
61	VOLUME – IV SCOPE OF WORK	105	The proposed solution should be sized for 10,000 sustained EPS both respective companies BRPL & BYPL each.	Reuired 2 separte instance for BRPL & BYPL or need multi tenancy based Architcture?	2 separte instance for BRPL and BYPL
62	VOLUME – IV SCOPE OF WORK	106	Bidder needs to provide independent SOC operations for both companies BRPL & BYPL and needs to be run from respective company locations for L1 and L2 support. L3 support needs to be provided from bidder location.	This SOC personal will be seated in which locations/city in india?	SOC personal will be seated in Delhi location
63	VOLUME – IV SCOPE OF WORK	106	NA	All SOC componnets reuired to be in Single site HA along with DC DR Solution architcture?	All system components to be in HA at same place or other site and will be finalize at the time of deployment
64	VOLUME – IV SCOPE OF WORK	105	NA	If DC & DR Architcture is available? Is it required actice active architcture or Active passive architcture?	System should support Active-active and Active-passive both architcture and will be finalize at the time of deployment
65	VOLUME – IV SCOPE OF WORK	105	NA	Threat intelligence soution need to be implimented on-prim or Cloud solutions can be integrted with SOC components?	Both option are open. Bidder can choose.
66	VOLUME – III TECHNICAL SPECIFICATIONS	95	Threat Intel Platform	Can we get the assest detailed inventory for SOC log sources	Will be provided to be bidder which is finalized by bidding process
67	VOLUME – IV SCOPE OF WORK	105	NA	How many use cases are needed as part of SIEM Implimentation?	This solution is going to be implemented for cyber security purpose and we do not want to limit it with any numbers.
68	VOLUME – IV SCOPE OF WORK	105	NA	How many Playbook are needed as part of SOAR Implimentation?	This solution is going to be implemented for cyber security purpose and we do not want to limit it with any numbers.
69	SCOPE OF WORK	Page 6 of 13 (page109)	Ticketing system for SIEM/SOAR incidents	Please clarify, Ticketing System(ITSM) shall be in customer scope. Bidder will not provide any type of Ticketing System.	Clause is well explanatory. No change in clause
70	SCOPE OF WORK	Page 6 of 13 (page109)	Incident detection, response and handling Incident triaging and Escalation management processes 4) Incident response (IR) is responsible for managing incidents as they occur, and communicating security requirements to the organization in the case of a significant data breach.	Please clarify, any kind of Digital Forensic Incident response is out of scope from Bidder scope.	All incidents response and handling including forensic needfs to be taken care by the bidder.
71	Technical Specification SIEM+SOAR+UEBA	Page 6 -36 (Page73)	SoC solution must be dedicated on premise solution and support IT and OT	SIEM+SOAR+UEBA, deployment method will be on virtual environment. Bidder will provide the sizing with data retention requirement. Customer has to provide virtual infra till end of the project.	All hardware and software requirement for the solution needs to be taken care by the bidders.

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
72	ITB 2.01Technical Criteria	Page4 of 16 (Page6)	Bidder must have at least 3 deployments for 20000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period ending bid submission date) for proposed SIEM solution or Must have at least 1 deployment for 75000 or more EPS installation in Govt sector, power sector, energy, BFSI or critical sector (period ending bid submission date) for proposed SIEM solution	Please decrease the 20000 EPS installation criteria to 10000 EPS installation criteria. As per TS SIEM EPS requirement is 10000 EPS and 1000 EPS is initial.	No change in RFP clause
73	2.01 Technical Criteria	Page 5	The Bidder should be a Managed Security Service Provider (MSSP) having its own Security Operations Centre (SOC) operating since last 5 years from the date of bid submission, from where it is providing services to different customers	**We request to dilute this clause. Experience of building and maintaining minimum 02 SOC's for customer should be considered as relevant qualification as the RFP scope is to build and maintain SOC for BYPL & BRPL and not for Managed Security Service Provider (MSSP) in Bidder SOC setup OR Allow Consortium to bid with one partner having the expericne of MSSP**	No change in the RFP clause
74	Technical Criteria Point 5		Bidder must have at least 3 deployments for 20000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period endingbid submission date) for proposed SIEM solution or Must have at least 1 deployment for 75000 or more EPS installation in Govt sector, power sector, energy, BFSI or critical sector (period ending bid submission date) for proposed SIEM solution	Bidder or OEM must have at least 2 deployments for 50000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (periodending bid submission date) for proposed SIEM solution or Must have at least 1 deployment for 75000 or more EPS installation in Govt sector, power sector, energy, BFSI or critical sector (period ending bid submission date) for proposed SIEM solution	No change in the RFP clause
75	Technical Specifications - SIEM General Requirement	Pg 73, point 10	The solution should support log collection, correlation and alerts for the number of devices mentioned in scope.	Please provided device inventory in scope	**Amended Clause:** The solution should support log collection, correlation and alerts for all the log sources.
76	Log Management	Pg 75, point 24	Log Management Performance: The proposed solution should have event handling capacity with low capacity incremental blocks.	These are specific to specific OEM, request to please remove as our proposed OEM is not complying.	**Amended Clause:** Log Management Performance: The proposed solution should have event handling capacity with low capacity incremental blocks or any other equivalent
77	Event and Log collection	Pg 76, point 37	The solution should provide time based and forward feature at each log collection point.	Revised clause proposed: The solution should provide device / time / event / IP based / and forward feature at each log collection point.	**Amended Clause:** The solution should provide device / time / event / IP based / and forward feature at each log collection point.
78	Correlation	Pg 78, point 65	The solution must support the ability to correlate against vulnerability assessment tool.	Our proposed solution will meet this requirement via SOAR. Pls confirm if it will be acceptable?	OK
79	Correlation	Pg 79, point 74	The system should provide the capability for correlate and identify zero-day threats on the network.	Amendment Requested - The system should provide the capability for correlate and identify zero-day threats on the network**, with the help of logsource EDR,WAF, IPS and VA tools, etc.**	No change in the RFP clause

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
80	Reporting	Pg 84, point 120	The solution should provide an integrated case management system which should ensure independent investigation eliminating the risk of possible intervention of administrator.	Our proposed solution will meet this requirement via SOAR. Pls confirm if it will be acceptable?	OK
81	UEBA	Pg 96, point 4	The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc.	These are specific to specific OEM, request to please remove as our proposed OEM is not complying.	No change in the RFP clause
82	UEBA	Pg 96, point 13	Uses self-learning behavioral analysis to dynamically model each device, probabilistically identifying any anomalous activity that falls outside of the device’s normal pattern of life.	Uses self-learning behavioral analysis to dynamically model each device/ **User**, probabilistically identifying any anomalous activity that falls outside of the device’s normal pattern of life.	**Amended Clause:** Uses self-learning behavioral analysis to dynamically model each device/user, probabilistically identifying any anomalous activity that falls outside of the device’s normal pattern of life.
83	UEBA	Pg 96, point 16	Flexibility to configure rolling window of period for behavior profiling	We are proposing Dynamic rolling window	Ok
84	UEBA	Pg 96, point 21	The solution should be able to automatically identify and classify users and entities (i.e. devices, applications, servers, data, or anything with an IP address)	The solution should be able to automatically identify and classify users and entities (i.e. devices, process, servers, resources, data, action, user or anything with an IP address)	No change in the RFP clause
85	UEBA	Pg 97, point 33	Sensitive data leakage: User manipulates http request / response parameter to download sensitive data	Our proposed OEM can achieve this functionality if BSES shall provide alerts from ADC/ WAF.	Ok
86	UEBA	Pg 97, point 36	The proposed UEBA solution must include rule configuration management capabilities. It should allow users to create rules for entity mapping and profiling, provide the rule descriptions, mark the severity of alerts, select a risk category and tag configuration to generate ticket, schedule a mail etc.	This is specific to specific OEM, request to please remove as our proposed OEM is not complying.	No change in the RFP clause
87	NDR Functional Requirements	Pg 102, point 4.33	The Proposed solution should detect policy violations.	Pls remove this point	**Amended Clause:** The Proposed solution should detect policy/ pattern violations.
88	NDR Functional Requirements	Pg 102, point 4.34	Policy Violation detection rules should be modifyble to include Layer 7 details.	Pls remove this point	**Amended Clause:** Policy/ Pattern Violation detection rules should be modifyble to include Layer 7 details.
89	NDR Functional Requirements	Pg 102, point 4.35	The solution should provide a statistics based visualization for the better understanding of the policy based detection	Pls remove this point	**Amended Clause:** The solution should provide a statistics based visualization for the better understanding of the policy/ pattern based detection
90	NDR Functional Requirements	Pg 102, point 4.36	The system should able to provide the aggregated analysis for the policy violation and forensic	Pls remove this point	**Amended Clause:** The system should able to provide the aggregated analysis for the policy/ pattern violation and forensic
91	NDR - Integration	Pg 103, point 5.5	The solution should integrate with OpenLDAP, Microsoft Active Directory, RADIUS and DHCP to provide user Identity information in addition to IP address information throughout the system.	Pls remove this point	No Change in the RFP clause
92	NDR - Integration	Pg 103, point 5.6	The system should have a mechanism to consume external lists of known bad IP‟s and generate alerts on the same if connection is seen.	Pls remove this point	No Change in the RFP clause

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for “SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL.”

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
93	NDR - Integration	Pg 103, point 5.7	The NDR system should be able to integrate with external threat feeds.	Pls remove this point	No Change in the RFP clause
94	NDR - Integration	Pg 103, point 5.9	The solution should have native integration with CERT CMTX & NCIIPC Threat Feeds	Pls remove this point	No Change in the RFP clause
95	NDR - Reporting	Pg 103, point 6.1	Solution should have built-in various reports and can create custom reports like Executive report, detection life cycle report and Health reports etc.	Solution should have built-in/ integrated solution to fetch various reports and can create custom reports like Executive report, detection life cycle report and Health reports etc.	**Amended Clause:** Solution should have built-in/ intergrated solution to fetch various reports and can create custom reports like Executive report, detection life cycle report and Health reports etc.
96	Scope of Work	Pg 105, point 1.7	The proposed next gen SIEM solution should have the capability to compress the logs by at least 50% for storage optimization.	Following should be added in clause that compression ration of minimum 10:1 should be mentioned for storage.	No change in RFP clause
97	Scope of Work	Pg 106 , point 1.20	Next gen SIEM solution should be EPS based and must support logs from unlimited devices or sources	EPS based or Device based or Gb per day should be accepted.	Yes will be acceptable should support min 5000 device with unlimited EPS count. (device should have 50% servers, 25% networ/routing, 25% firewall and security devices)
98	Scope of Work	Pg 106 , point 1.22	No Events should be dropped during Spikes, even if license limits gets exceeded: The proposed solution must not, under any circumstances, drop incoming events.	To be updated as follows: Solution should used accomadated unused EPS counts to avoild event drops during spikes, even if license limits gets exceeded: The proposed solution must not, under any circumstances, drop incoming events.	No change in RFP clause. Bidder / OEM needs to check how they achive this.
99	Pre Qualification	Pg 6, point 5	Bidder must have at least 3 deployments for 20000 EPS installation, each in Govt sector/ power sector/ energy/ BFSI/ critical sector (period ending bid submission date) for proposed SIEM solution or Must have at least 1 deployment for 75000 or more EPS installation in Govt sector, power sector, energy, BFSI or critical sector (period ending bid submission date) for proposed SIEM solution	In Documents required if OEM self certification with client details and project details mentioned then it is to be accepted.	Clause is self explanatory and to be read along with documents to be submitted
100	Award Decision	Pg 10, point 4.05	Rate shall remain FIRM till the validity of the Contract.	USD fluctuation and OEM upflift to be acceeomodated by BSES	Tender Condition shall prevail
101	Terms of Payment - For SOC Operations, Pg 47	Pg 47, point in SOC operations	Bidder require to submit 10% of PBG of Contract value for full contract period.	PBG referred here is same which is already asked in ITB at pg 18 and pn pg 50 as well for 10% of PO value for entire contract value. Pls clarify so as to avoid duplicacy.	Referred PBGs are same.

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for "SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL."

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
102	Indemnification, Pg 55	Pg 65, point	Notwithstanding contrary to anything contained in this RFQ, Supplier shall at his costs and risks make good any loss or damage to the property of the Purchaser and/or the other Supplier engaged by the Purchaser and/or the employees of the Purchaser and/or employees of the other Supplier engaged by the Purchaser whatsoever arising out of the negligence of the Supplier while performing the obligations under this contract.	Indemnification is requested to be capped till contract value only.	Tender Condition shall prevail
103	Termination for convenience of Purchaser	Pg 55, point 34	Purchaser at its sole discretion may terminate the contract by giving 30 days prior notice in writing or through email to the Supplier.	Please remove this point. Termination for convinience is not applicable asonly material breach termination can be accepted in suc contracts globally and as per industrial practice.	Tender Condition shall prevail
104	Limitation of Liability	Pg 56, point 38	Liability of supplier is capped at contract value in RFP	Request to please modify the clause and limit supplier value to implementation services amount only. As a supplier we cannot own liability of product functioning as it is taken care by OEM.	Tender Condition shall prevail
105	Commercial Qualification Criteria	Pg 7, point 2.02 - 8	The Bidder should have a positive net worth in last three financial years (i.e. 2021-22, 2022-23, 2023-24). Bidder should furnish a Certificate from the Chartered Accountant (CA) for Net Worth.	It is requested to accept Balance Sheet/ copy of audited P&L account.	Tender Condition shall prevail
106	NDR	Pg 98, point 1.3	The proposed solution must support full packet capture and smart Capture.	The proposed solution must support full packet capture.	**Amended Clause:** The proposed solution must support full packet capture/ smart Capture.
107	NDR	Pg 99, point 2.3	The proposed solution must have the ability to natively monitor layer 7 traffic and perform deep packet inspection (DPI) without any 3rd party solution.		
108	NDR	Pg 103, point 7.8	The solution should offer country level traffic visibility and should have dedicated Country wise traffic dashboard.	Pls remove this point	No change in the RFP clause
109	UEBA	Clause 52, Pg 98	Use of supervised machine learning algorithms	Please modify to unsupervised machine learning algorithms	**Amended Clause:** Use of supervised/ unsupervised machine learning algorithms
110	Scope of Work for Security Operations Center	Clause 1.12, Pg 105	The proposed solution must support 1000+ data sources with predefined parsing/normalizations rules out of the box.	The proposed solution must support 1000+ datasources/keywords with predefined parsing/normalizations rules out of the box.	**Amended Clause:** The proposed solution must support 1000+ datasources/keywords with predefined parsing/normalizations rules out of the box.
111	QUANTITY AND DELIVERY REQUIREMENTS	Pg.19-20, point 7	85-inch industrial LED panel/screen for SOC with 2x2 screen splitter, 5 yrs warranty		**Amended:** 85-inch industrial LED panel/screen for SOC with 2x2 screen split funtion with seprate data on each split window, 5 yrs warranty

NIT NO. CMC/BY/24-25/RS/SkS/APT/48 [RFx No. 2200000076] for "SUPPLY & IMPLEMENTATION OF SOC SOLUTION INCLUDING TECHNOLOGIES SIEM, SOAR, UEBA, NDR/NBAD, THREAT HUNTING, THREAT INTELLIGENCE, INCIDENT MANAGEMENT FOR BYPL & BRPL."

Response/ Calrifications to the bidders per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
112	SIEM, Point 79	13	The solution must leverage both Supervised / Un-supervised Machine learning techniques without signatures		**Amended Clause:** The solution must leverage both Supervised / Un-supervised Machine learning or deep learning or equivalent techniques with or without signatures
113	UEBA, point 36	30	The solution must have the capability to perform a continuous evaluation of threat actor, and can cluster the behaviour and impacted entities, it can then build a baseline with ML capabilities and this baseline forms the input to detect sophisticated attacks. This process takes input from both internal and external threat intelligence sources		**Amended Clause:** The solution must have the capability to perform a continuous evaluation of threat actor, and can cluster the behaviour and impacted entities, it can then build a baseline with ML/ deep learning/ equivalent capabilities and this baseline forms the input to detect sophisticated attacks. This process takes input from both internal and external threat intelligence sources
112	NDR		New Addition		NDR device should be capable to support 10Gbps traffic throughput from day one without any hardware upgradation and should have 4 x 1/10G (copper) traffic capture/ monitoring ports and 2 x 1G management ports along with 5Gbps license from day one. Full packet capture needs to be planned with 7 days retention of PCAP files.