S No	Query Type Technical/ Commercial	Page No	Clause No	BRPL Clause	Bidder Query	BRPL REPLY
1	Technical	47	Scope and Technical Specifications	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)	Kindly requesting to amend this clause as " 1.14. The Platform must include log management, NG SIEM, Host Forensics, 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 with no additional 3rd party solution) "	**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
2	Technical	48	Scope and Technical Specifications	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	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
3	Technical	73	Technical Specification	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
4	Technical	86	Technical Specification. Sr. No.98	SOAR should have an integrated Threat Intelligence Platform (TIP) and should Facilitate importing and parsing structured and unstructured intelligence documents- Structured/finished intelligence analysis reports (.txt, .PDF); Automatically ingest email lists with threat information; Formatted CSV Files, XML-based structured intelligence –	We request to kindly amend the clause for maximum participation and separateThreat Intelligence platform (TIP) from SIEM & SOAR. So that be able to get best available product. **Justification:-** SIEM & SOAR is the platform that helps an organization to repond to recognized threats and vulnerabilities, while TIP is the solution to procatively detect and categorize threats using paid & unpaid feeds.Hence these are both separate platforms and not a single solution. There are standard protocols and formats for integrating TIP solution with SIEM & SOAR. Hence to get the best capabilities it is advised to separate TIP from SIEM & SOAR solutions which allows both independent and integrated solutions to participate in the tender. Moreover The Independent Threat Intelligence Platform (TIP) offers enhanced capabilities for integrating and analyzing threats from various external feeds, providing its own risk score to help users better understand incoming threats. Additionally, this TIP can seamlessly integrate with all external feeds, including CERT-In and NCIPC, as well as can integrate with all network security devices.	Tender condition prevails
5	Technical	8	Technical QR Sr. No-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	We kindly request that the clause be amended to promote maximum participation and separate Threat Intelligence platform(TIP) from SIEM & SOAR. This will help in selecting the best available product. TIP OEMs (Make in India) should be allowed to participate with their products, provided they meet the technical compliance outlined in the RFP, as the government has emphasized supporting products under the Make in India initiative.	Tender condition prevails

6	Technical	7	Clause 2	The Bidder should be a Managed Security Service Provider (MSSP) having its own Security Operations Centre (SOC) operating since last 4 years from the date of bid submission, from where it is providing services to different customers	Since the scope of RFP is to setup SOC center. This clause may be deleted	Tender condition prevails
7	Technical	7	Clause 4	Bidder should have experience of SOC operations for minimum 5 SOC customers in last 4 years in Govt sector,power sector, energy, BFSI or critical sector.	Clause may be amended as - "Bidder should have experience of deployment of SOC for minimum 5 customers in last 4 years in Govt sector, power sector, energy, BFSI or critical sector	Bidder should have experience in both SOC implementation and operations. With minimum 5 SOC customers in last 4 years in Govt sector,power sector, energy, BFSI or critical sector.
8	Technical	8	Clause 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 I deployment for 75000 or more EPS installation in Govt sector, power sector, energy, BFSI or critical sector (periodending bid submission date) for proposed SIEM solution	Clause may be amended as - 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 SIEM solution or: Must have at least 1deployment for 75000 or moreEPS installation in Govt sector,power sector, energy, BFSI or critical sector (period ending bidsubmission date) for SIEM solution	Tender condition prevails
9	Technical	7	Clause 2	The Bidder should be a Managed Security Service Provider (MSSP) having its own Security Operations Centre (SOC) operating since last 4 years from the date of bid submission, from where it is providing services to different customers	We are MMSP but do not have our own Security Operation Centre (SOC). We can support through our Partner SOC & our own SOC is going live soon.	Tender condition prevails
10	Commercial	8	ii	The bidder should have net worth of Rs 3 Crore as on the last day of the preceding financial year on the date of bid submission. The bidder shall submit the Certificate of Net Worth duly certified by Chartered Accountant for the last financial year i.e. FY 2023- 24.	Requesting to kindly replace this clause as below- The bidder should have positive net worth as on the last day of the preceding financial year on the date of bid submission. The bidder shall submit the Certificate of Net Worth duly certified by Chartered Accountant for the last financial year i.e. FY 2023- 24.	Tender condition prevails
11	Commercial	8	iii	Bidder must provide proof of having solvency of an amount equal to Rs 2 Crore from any nationalized/ scheduled commercial bank. It should not be older than 30 days from the date of submission of Techno-Commercial bid.	We are in process of preparing a solvency proof document of 2.5 Crore for BRPL "implementation of OT tool" tender. Can we provide the same for both tenders since the buyer for both tenders is same.	Solvency should not be older than 30 days from the date of submission of Techno-commercial bid.
12	Technical	50	m	Bidder should be MSSP having SOC 2, Type II certified. Certified report – 1st page of report to be submitted.	Requesting to allow bidders with ISO/IEC 27001 Certificate to qualify in this clause. Once the bid is awarded we will apply for SOC 2, Type 2 certificate	SOC 2 Type II Certificate is optional

13	Technical	86	Technical Specification. Sr. No.98	SOAR should have an integrated Threat Intelligence Platform (TIP) and should Facilitate importing and parsing structured and unstructured intelligence documents- Structured/finished intelligence analysis reports (.txt, .PDF); Automatically ingest email lists with threat information; Formatted CSV Files, XML-based structured intelligence –	We request to kindly amend the clause for maximum participation and separateThreat Intelligence platform (TIP) from SIEM & SOAR. So that be able to get best available product. **Justification:-** SIEM & SOAR is the platform that helps an organization to repond to recognized threats and vulnerabilities, while TIP is the solution to procatively detect and categorize threats using paid & unpaid feeds.Hence these are both separate platforms and not a single solution. There are standard protocols and formats for integrating TIP solution with SIEM & SOAR. Hence to get the best capabilities it is advised to separate TIP from SIEM & SOAR solutions which allows both independent and integrated solutions to participate in the tender. Moreover The Independent Threat Intelligence Platform (TIP) offers enhanced capabilities for integrating and analyzing threats from various external feeds, providing its own risk score to help users better understand incoming threats. Additionally, this TIP can seamlessly integrate with all external feeds, including CERT-In and NCIPC, as well as can integrate with all network security devices.	Tender condition prevails
14	Technical	8	Technical QR Sr. No-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	We kindly request that the clause be amended to promote maximum participation and separate Threat Intelligence platform(TIP) from SIEM & SOAR. This will help in selecting the best available product. TIP OEMs (Make in India) should be allowed to participate with their products, provided they meet the technical compliance outlined in the RFP, as the government has emphasized supporting products under the Make in India initiative.	Tender condition prevails
15	Technical	7		Bidder should have experience of SOC operations for minimum 5 SOC customers in last 4 years in Govt sector, power sector, energy, BFSI or critical sector. Customer names on bidder letter head along with person's name, contact details like mail id and phone numbers to be provided.	We request you to please relax the point to Bidder/ OEM	Tender condition prevails
16	Technical	7		Bidder should have experience of SOC operations for minimum 5 SOC customers in last 4 years in Govt sector, power sector, energy, BFSI or critical sector. Customer names on bidder letter head along with person's name, contact details like mail id and phone numbers to be provided.	We request you to please relax the point to Bidder/ OEM	Tender condition prevails
		53	2.3	High level Deliverables.	Request BRPL Rajadhani to amend the clause as " The resolution is on the best effort basis".	Tender condition prevails
		Page 31 of 36	1.4	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.	Tender condition prevails

		Page 32 of 36	3.2	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.
		Page 32 of 36	3.4	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.
		Page 33 of 36	3.10	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=Egxnd3Mtd2l6LXNIcnAiF2Npc2NvIG5zZWwgcHJvcHJpZXRhcnkgMgUQIRigATIFECEYoAEyBRAhGKABSJIlUOwBWJpGcAF4AZABAJgBqAOgAfosqgEIMi00LjExLjK4AQPIAQD4AQGYAgygAtEdwgIKEAAYsAMY1gQYR8ICBhAAGBYYHsICCxAAGIAEGIYDGIoFwgIIEAAYgAQYogTCAgcQIRigARgKwgIEECEYFZgDAIgGAZAGBJIHCTEuMC4yLjcuMqAHnzw&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. Tender clause prevails.
		Page 33 of 36	3.11	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
		Page 33 of 36	3.12	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.
		Page 36 of 36	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	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
		50	Scope of Work Point m.	Bidder should be MSSP having SOC 2, Type II certified. Certified report – 1st page of report to be submitted.	Request you relax this clause.	SOC 2 Type II Certificate is optional

				Suggested points to be added	The solution must distinguish between similar devices based on unique fingerprints (including unmanaged & IOT) and provide commonality & frequency analysis for each such fingerprint to minimize the false positive rate. Must automatically group similar devices together based on a combination of fingerprints, provide an explanation of the similarity, and identify packet captures corresponding to that fingerprint for forensic and outlier analysis. Justification: This is critical functionality of the NDR solution **Justification:** This is critical functionality of the NDR solution	Not to be included.
				Suggested points to be added	The solution should support and provide examples at a minimum, all of the following data science methods. Details with examples on how each of these data science methods are used should be provided and demonstrated as part of the proof of concept evaluation if required. ● Supervised machine learning ● Unsupervised machine learning ● Deep neural networks ● Belief propagation ● Multi-dimensional clustering ● Decision tree classification ● Outlier detection **Justification:** This is critical functionality of the NDR solution	These are optional not mandatory
		89	UEBA Technical Specification Point No.52	Use of supervised machine learning algorithms	Request BRPL to Amend the point as follow"Use of supervised/Unsuprevised machine learning algorithms	**Ammeded:** Use of supervised/Unsuprevised machine learning algorithms
		47	Scope and Technical Specification	The proposed solution must support 1000+ data sources with predefined parsing/normalizations rules out of the box.	Request BRPL to remove this clause.	The proposed solution must support min400 data sources with predefined parsing/normalizations rules out of the box.
		47	Scope and Technical Specification	The Platform must include log management, NG SIEM, Host Forensics, UEBA, NDR, File Integrity Monitoring, Security Analytics, Big Data Analytics, Security Automation and	Request BRPL to Amend the point as "- 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).	Accepted
		94	Scope and Technical Specification - NDR	5.4: The solution should have capability to instruct network security devices such as firewalls to block certain types of traffic, quarantine the host, etc.	This is a role of SIEM or SOAR solution, hence we request this requirement to be moved to SIEM or SOAR.	Refer Corrigendum-II
		95	Scope and Technical Specification - NDR	7.4: The solution should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm.	This is a role of SIEM or SOAR solution, hence we request this requirement to be moved to SIEM or SOAR.	Refer Corrigendum-II
	Commercial	8	i of Financial QR	The average annual turnover of the Bidder, in the preceding three (3) financial years (i.e., FY23-24, FY22-23 & FY21-22) should not be less than Rs 11 Crore. The bidder shall submit the Annual Turnover Report of the last 3 FYs duly certified by a Chartered Accountant. The Turnover certificate must have UDIN Number.	Request to read clause as "The average annual turnover of the Bidder, in the preceding three (3) financial years (i.e., FY23-24, FY22-23 & FY21-22) should not be less than Rs 11 Crore. The bidder shall submit the Annual Turnover Report of the last 3 FYs duly certified by a Chartered Accountant."	Tender condition prevails
	Commercial	8	ii of Financial QR	The bidder should have net worth of Rs 2 Crore as on the last day of the preceding financial year on the date of bid submission. The bidder shall submit the Certificate of Net Worth duly certified by Chartered Accountant for the last financial year i.e. FY 2023-24. The Net worth certificate must have UDIN Number.	Rwequest to read clause as "The bidder should have net worth of Rs 2 Crore as on the last day of the preceding financial year on the date of bid submission. The bidder shall submit the Certificate of Net Worth duly certified by Chartered Accountant for the last financial year i.e. FY 2023-24."	Tender condition prevails

Commercial	8	iii of Financial QR	Bidder must provide proof of having solvency of an amount equal to Rs 1.5 Crore from any nationalized/ scheduled commercial bank. It should not be older than 30 days from the date of submission of Techno-Commercial bid.	Request to remove this clause.	Tender condition prevails
Technical	7	4 of Technical QR	Bidder should have experience of SOC operations for minimum 5 SOC customers in last 4 years in Govt sector, power sector, energy, BFSI or critical sector. Customer names on bidder letter head along with person's name, contact details like mail id and phone numbers to be provided.	Request to read clause as "Bidder should have experience of SOC/MSS/SIEM operations for minimum 5 customers in last 7 years in Govt sector, power sector, energy, BFSI or critical sector, Enterprise Sector. Customer names on bidder letter head along with person's name, contact details like mail id and phone numbers to be provided."	Bidder should have experience in both SOC implementation and operations. With minimum 5 SOC customers in last 4 years in Govt sector,power sector, energy, BFSI or critical sector.
Technical	8	5 of Technical QR	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	Bidder/OEM must have at least 3 deployments for SIEM installation, in Govt sector/power sector/ energy/ BFSI/ critical sector/ Enterprise Sector. (period ending bid submission date) for SIEM solution	Tender condition prevails
Technical	8	5 of Technical QR	a. Purchase Order copies b. Performance Certificate/ Completion certificate/ Invoice Copies If bidder is an authorized partner of OEM, credentials of OEM shall be considered.	Request to accept PO copies or Performance Certificate or Completion Certificate.	Tender condition prevails
Technical	9	Commercial	Bidder to submit UDIN based CA Certificate showing NIL dues towards Statutory Liabilities, including GST, Taxation, PF, ESI, or any other dues Statutory in nature for the period upto 30.06.2024, herein collectively called as "Statutory dues" and there is no liability over the bidder relating to deposition of such statutory dues.	Request to remove this clause.	Tender condition prevails
Commercial	9	Other Requirements: b (iii)	Detail of Banks & Fund & Non fund based Credit limit		Tender condition prevails
Commercial	9	Other Requirements: b (xi)	Work order copies along with performance certificates in support of relevant experience	Request to accept only PO copies also.	Tender condition prevails
Commercial	9	Other Requirements: b (xii)	Turnover certificate issued by CA (along with UDIN no.) for the last three Financial Years.	Request to accept only audited Balance sheet and P&L Account statement. Annual Turnover Report of the last 3 FYs duly certified by a Chartered Accountant	Tender condition prevails
Commercial	30	8.2 (f)	Two (02) copies of Supplier's transporter invoice duly receipted by BRPL Store & Original certificate issued by BRPL confirming receipt of the subject material at Store/Site and acceptance of the same as per the provisions of the contract.	Is this applicable?	Tender condition prevails
Commercial	36	26	INDEMNIFICATION 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 prevails

Commercial	40	9	INDEMNITY:	Indemnification is requested to be capped till contract value only.	Tender condition prevails
Commercial	45	1.3	TERMINATION BY COMPANY FOR CONVENIENCE	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 prevails
Commercial	98	8 of PRICE FORMAT	Price Variation Clause: The prices shall remain firm during the entire contract period.	USD fluctuation and OEM upflift to be acceomodated by BSES. Since the product and solutions are imported so US dollar fluctions play a very important role. So USD incremental fluctuations to be paid and base price will be kept firm. Secondly this is a security product and all security OEM have industry standard uplift to be paid by BSES.	Tender condition prevails
Technical	89	52	Use of supervised machine learning algorithms	Please change "supervised" to unsupervised Unsupervised machine learning is better that Supervised machine learning and supervised machine learning is specific to one OEM.	**Amended:** Use of supervised/Unsuprevised machine learning algorithms
Technical	47	1.12	The proposed solution must support 1000+ data sources with predefined parsing/normalizations rules out of the box.	Please change “1000+ datasource with” 1000+ rules	The proposed solution must support min400 data sources with predefined parsing/normalizations rules out of the box.
Technical	50	2.1 m)	Bidder should be MSSP having SOC 2, Type II certified. Certified report – 1st page of report to be submitted.	Pls remove this point, as entire team seating your on-premises no point of SOC2	SOC 2 Type II Certificate is optional
Technical	50	2.1 n)	Bidder should have knowledge/ experience of IT and OT-ICS domains (Optional). BRPL will provide the access of security devices like WAF, SIEM and SOAR etc installed at BRPL premise and bidder needs to monitor and manage its operations.	Pls remove WAF from devices for manage it operations	NO change in RFP. Clarification: WAF logs to be integrated as one of inputs.
Technical	52	2.2	TEAM STRUCTURE	Need to increase Team size for SIEM SOAR Operations	Tender condition prevails
Technical	53	2.3	HIGH LEVEL DELIVERABLES	Resolution shall be on a best effort basis, request to remove resolution timeline	Tender condition prevails
Technical	63	10	The solution should support log collection, correlation and alerts for the number of devices mentioned in scope.	Please provided device inventory MAKE & MODEL in scope	Device Details to be provide post singing NDA
Technical	57	2.5	Maximum penalty in a quarter will be capped to 10% of quarterly SOC operation charges. Bidder shall not be responsible for SL impact where the delay is not attributable to the bidder. All such cases have to be adequately evidenced.	Request to change clause as "Maximum penalty in a quarter will be capped to 5% of quarterly SOC operation"	Tender condition prevails
Technical	59	6.1	System warranty will be started after installation, commissioning and Go-live of SIEM Solution. Timeline will be six months or go-live whichever is earlier.	Number of Device are missing kindly share device inventory MAKE & MODEL in scope for define timeline	Device Details to be provide post singing NDA
Technical	48	1.26,	Provide system landscape design along with server, storage. Server and storage sizing should be done keeping 20000 EPS and raw log retention for at least 6 months. Appropriate Hardware (server/storage) required should be provided by the bidder along with all required licenses.	Log retention for at least 6 months but asking on Page no 53, clause 2.3 Logs of any duration of one year as asked by BRPL: within 24 hours, need clarity for retention time to adhere deliverables	Log retention period is 180 days
Technical	89 of 121	Volume III, Technical Specifications. Network Detection & Response 1.7	Proposed NDR systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	For functionality of NDR, there may be a requirement to create port mirror on the switches, routers or any existing network infrastructure. We request that this clause be amended to permit dependency up to the extent of fulfillment of the requirement of traffic acquisition by way of port mirror or setting up flow collector.	Port mirror will be provided

Technical	90 of 121	Volume III, Technical Specifications. Network Detection & Response 3.2	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.	To capture packets effectively, port mirroring on switches or routers may be required besides other devices that have the capability. Therefore, this dependency exists on existing infrastructure. Therefore, we request that either this clause be amended to include packet capture dependency on switches or routers or, requirement 1.7 be edited to widen the scope of dependency on existing infrastructure.	**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.
Technical	91 of 121	Volume III, Technical Specifications. Network Detection & Response 3.10	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	A couple of earlier requirements indicate that NDR should work using DPI and full packet capture. Flow collector is a separate solution and depends on the ability of flow sensor (usually a router/switch) to provide application visibility to L4 service assignment or custom assignment only and it does not include L7 application visibility that DPI provides. Please identify what is needed from the two - flow collector for flow sensors or deep packet inspection?	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. RFP Clause prevails.
Technical	91 of 121	Volume III, Technical Specifications. Network Detection & Response 3.12	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.	The Nat Gateway (CGN) or Firewall should be capable of generating flow data for address and port translation. Please confirm if this capability exists and the format of flow data delivery - clear-text log, IPFix or, NetFlow?	**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.
Technical	93 of 121	Volume III, Technical Specifications. Network Detection & Response 4.19	The solution should support active scanning of specific enterprise assets in addition to passive profiling of devices on the network.	Please indicate if the buyer is okay to implement agents on hosts for which active scanning is desired. Also, do indicate an estimated number of assets that require such scanning.	Active scan can be kept with defined polling rate, without hampering operation.
Technical	New Clause	New Clause	Does NDR sensor required in HA along with Central management?		SOC solution (SIEM, SOAR, NDR) will be in HA, For NDR, only central mgmt, central mgmt / correlation tobe in HA. Packet capture will not be in HA.
	86	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.
	87	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
	87	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.

	87	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
	89	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.	**Ammeded:** Use of supervised/Unsuprevised machine learning algorithms
	47	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 with no additional 3rd party solution)
	48	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