Corrigendum 1

IMPLEMENTATION OF OT SECURITY ''REAL THREAT & VULNERABILITY MANAGEMENT SYSTEM" IN BYPL
NIT NO: CMC/BY/24-25/RS/SkS/APT/51
[RFx Number: 2200000084]

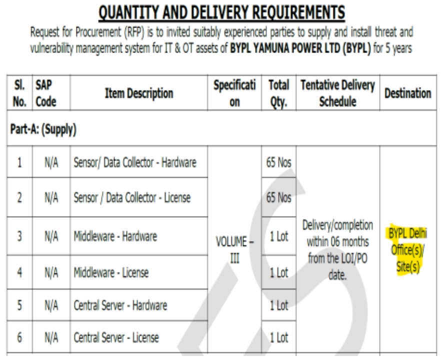
Calrifications to the per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
1	2.01	6	The Bidder must have completed minimum three (03) similar full cycle implementation of offered OT security systems in the last five (05) years prior to the date of bid submission of which at least one (01) implementation should be in Power/ Energy/ Utility sector.	1. Since OT IDS technology is pretty much new in india the implementation we have done is for airport which is decleared as critical infrastructure by indian government, here we have also covered electricity substations which are dedicated for airports. would this creadential be sufficient? 2. We have done few implementation globally Could you please consider as technology is same. 3. Few Creadentials might be from different OEM as we work with multiple OT IDS OEM's, request you to consider this as well.	Mix of Indian and Global experience will consider but out of 3 atleast one should be Indian experience in Power/Energy/Utility sector
2	2.01	6	The Bidder should have minimum Five (5) years' experience in providing at least 03 supply, implementation and technical support services for OT deployment engagements in Govt sector, power sector, energy, BFSI or critical sector and Out of which one (01) engagement should have at least 15 sites or 1000 assets being monitored and Should have at least two (02) in-house OEM and one (01) IEC62443 certified technical expertise on its payroll	Same as above point	Mix of Indian and Global experience will consider but one should be Indian experience. Certified expertise resopurce should be in India.
3	5.06	44	Purchaser reserves the right to send any material being supplied to any recognized laboratory for testing, wherever necessary and the cost of testing shall be borne by the Bidder. In case the material is found not in order with the technical requirement/specification, the charges along with any other penalty that may be levied are to be borne by the bidder.	How many devices will be sent to laboratory for testing and the location of Lab?	Bidder need to provide all testing certificate from Indian laboratory as stated in MoP order on CEA (Cyber Security in Power Sector) Guidelines, 2021 If applicable for the devices under this tender scope.
4	12.01	48	**For OT Security Operations:** Payment of SOC (Operation service) shall be after the go live after submission of PBG separately for Soc amount. Note: Milestone payments shall be made in full upon the successful completion of the milestone.In the event that only a minor portion of a milestone is not fully completed, invoicing for partial payment of the milestone will be entirely to BYPL discretion. **Payment terms shall be within 45 days** from receipt of invoice supported by BYPL certification of completion of milestone.	Kindly confirm OT monitoring will be done through IDS/CMC & not through SIEM ?	Yes through the system which bidder will be deploying through this NIT

Corrigendum 1

IMPLEMENTATION OF OT SECURITY ‘’REAL THREAT & VULNERABILITY MANAGEMENT SYSTEM” IN BYPL
NIT NO: CMC/BY/24-25/RS/SkS/APT/51
[RFx Number: 2200000084]

Calrifications to the per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
5	12.01	46	**For Supply of Equipment’s (Part-A):** **MS-1**: 70% of contact value for of Pricing schedule shall be released subject to fulfillment of following pre-requisites: (i) Submission of detailed project schedule. (ii) Submission and approval of detailed engineering documents, Design Documentation for Hardware & Software System, List of Deliverables. (iii) Delivery and installation of required hardware and licenses. (iv) Submission of 10% PBG of part A for entire period of warranty period. **MS-2**: 20% of contact value of Pricing schedule shall be released subject to fulfillment of following pre-requisites: (i) Implementation Closure: which includes integration with sites mentioned in the Scope of the RFP and also integration with the other solutions procured in this RFP, i.e. UAT, and receiving sign off. (ii) Closure of all exceptions including Availability of application, Applications tuning competition, (iii) Approval of Administration & Operator’s User’s Manual, (iv) Documentation & training. **MS-3**: 10% of contract value for shall be released after 1 months of successful system run without any issues.	Payment of Hardware & Software needs to be released as per the PO terms e.g 30 days. As Installation of harware will take longer period based on other dependencies such as approval from system owners, site visit approval etc.	Refer note at Pg 48 (12.0 Terms of Payment and Billing)
6	26.01	52	**Penalty for Delay** If supply of items/equipments is delayed beyond the supply schedule as stipulated in the purchase order then the Supplier shall be liable to pay to the Purchaser as penalty for delay, a sum of 1% (one percent) of the basic (ex-works) price for every week delay of undelivered units or part thereof for individual milestone deliveries.	This clause needs to be excluded as delay may occur due to WAR situation in Israel. or any situation beyond our control. We will notify such condition if occurs.	Tender condition shall prevail.
7	26.01	52	The total amount of penalty for delay under the contract will be subject to a maximum of ten percent (10%) of the basic (ex-works) price of total undelivered units.	Based on our observations from other OT implementation projects, delays are typically caused by the customer not providing the necessary details and approvals on time. Therefore, we request a relaxation of this clause.	Any delay caused because of customer will be excluded from penalty
8		59	 **QUANTITY AND DELIVERY REQUIREMENTS** Request for Procurement (RFP) is to invited suitably experienced parties to supply and install threat and vulnerability management system for IT & OT assets of **BYPL YAMUNA POWER LTD (BYPL)** for 5 years Sl. No. / SAP Code / Item Description / Specification / Total Qty. / Tentative Delivery Schedule / Destination Part-A: (Supply) 1 / N/A / Sensor/ Data Collector - Hardware / VOLUME – III / 65 Nos / Delivery/completion within 06 months from the LOI/PO date. / BYPL Delhi Office(s)/ Site(s) 2 / N/A / Sensor / Data Collector - License / / 65 Nos 3 / N/A / Middleware - Hardware / / 1 Lot 4 / N/A / Middleware - License / / 1 Lot 5 / N/A / Central Server - Hardware / / 1 Lot 6 / N/A / Central Server - License / / 1 Lot	Usually, the bidder sends the device to a central location. The customer then delivers it to other locations because it's hard to get access to the premises. The standard delivery time for devices is 6-8 weeks.	All equipements need to be delivered at central place from where bidder will be moving it to different sites for installtion on their own expense.
9	3	65	Unloading at stores/sites shall be in vendor's scope.	Generally this needs to be in customers scope as obtaining permit/site pass is difficult process.	No change in clause. Clarification: Any permit/ site pass required for delivery/unloading will be arranged by customer.
10	3 (e)	78	System installed (Hardware and Software) at central should be in HA mode	In BOQ only 1 central device/IDS appliance is considered hence HA is not possible.	All deivices at central datacenter is to be in HA. Consider UOM in price bid as lot and not nos for part-A, 5 & 6 points of price bid.
11	Phase 4	78	Deploy the data diode at respective sites for integration with business network.	Is data diode also part of this project if yes then need to understand the network architecture and application of it. Proposed cost (6 cr) cant contain data diode cost.	Data diode is not part of the supply

Corrigendum 1

IMPLEMENTATION OF OT SECURITY ''REAL THREAT & VULNERABILITY MANAGEMENT SYSTEM" IN BYPL
NIT NO: CMC/BY/24-25/RS/SkS/APT/51
[RFx Number: 2200000084]

Calrifications to the per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
12	Phase 7	79	Provide access of the solution to the Site team and provide them training.	Operational/Knowledge transfer training will be arranged.	Yes, for Admin and user related training from OEM & Bidder
13	Phase 7	79	Operationalize the site and initiate 24x7 monitoring. Perform 24x7 monitoring of the OT Server.	According to RFP 2 resource (L1 in 8 hrs) are required for monitoring, with these resources 24*7 monitoring can not be achieved.	Monitoring will be in day time only in two shifts and shift timimngs will be finalize after vendor finalization.
14	7a (i)	80	**Authorization & Authentication:** Supports multi-factor authentication for admin activities	Almost all OT IDS Product supports the integration with MFA However, it does not contain direct capability without integration	Ok
15	14.1 (b)	84	Force majeure events including on site power failures.	How this will be tracked and documented?	Device should be capable to provide reason of restart like configuration change, power failure/restart etc
16			Useually OT IDS POC duration is max 30 days for a single site only	Please confirm if this is fine	OK
17	General Query		Required high level existing architecture of all sites for OT IDS design	Please provide the architectures	Can connect with technical team at given contacts in NIT
18	General Query		Are all 65 sites are centrally connected and not air-gapped?	Please confirm	Yes, all are centrally connected with OT data center
19	General Query		How many switches does not supports SPAN/RSPAN/ERSPAN	Please provide the quantity and locations	All switched support SPAN
20	General Query		Are there any Network switch available for OOB configuration?	If not available BYPL network team to arrange Management connectivity for all sites	Connectivity between site and Datacenter is in scope of BYPL
21	General Query		Are any sites connected via wireless technologies?	We need to check whether wireless technologies such as Zigbee, LoraWAN, wirelessHART etc. are being used in the plant.	No
22	General Query		Are there any air-gapped networks that need to be included in the security monitoring? If so, how many locations are there, and are IT switches available to provide management connectivity to IDS?	Please confirm	All locations had network switch available to provide management connectivity to IDS. Cable needs to be consider by the bidder.
23	General Query		Which OT protocols are being used?	Please confirm	IEC104, IEC103, 61850, MMS, MODBUS, Goose etc
24	General Query		Number of network switches used in network per site?	Please confirm	It varries site to site
25	General Query		Hardware vendors and model numbers of network switches?	Please confirm	Connect with technical team at given contacts in NIT
26			Asset Discovery Scan: a) Data Gathering Techniques: Passive scan, Safe Active query (Manual), Active Directory etc. Able to perform passive network traffic analysis and discover of all devices IT, OT, IOT, both with and without IP (serial connected devices using Modbus protocol). provide portable collectors to gain visibility of assets connected in unmanaged switch environment where passive monitoring is not feasible.	Asset Discovery Scan: a) Data Gathering Techniques: Passive scan, Safe Active query (Manual), Active Directory etc. Able to perform passive network traffic analysis and discover of all devices IT, OT and IOT. provide portable collectors to gain visibility of assets connected in unmanaged switch environment where passive monitoring is not feasible.	Non IP devices are Optional
27			Asset Scripts: provision to write scripts to discover and enrich the asset profiles. provide a detailed documentation on creating the scripts to OT administrator to write the code.	Need clarity on this.	This will enable us to write a small script for any undiscover protocol to get them discover
28			Vulnerability Assessment: Should be able to perform VA of all IT & OT connected devices to network., all version of OS.	Need clarity on this.	Yes
29			For each CVE, active threat intelligence shall be provided indicating following at a minimum: a. Exploit Code Maturity, b. Vulnerability Age & Product Coverage, c. Threat Intensity By Malicious Actors, d. Threat Activity Regency, And Sources Of Threat Information.	For each CVE, active threat intelligence shall be provided indicating following at a minimum: a. Threat Intensity By Malicious Actors, b. Threat Activity Regency, And Sources Of Threat Information.	No change in the RFP Clause
30			Able to perform vulnerability assessment of assets in layer 1,2,3 as per Purdue model.	Need clarity on this.	Clause is clear. VA findings should be mapped as per Purdue model layers
31	RFP Page No. & Clause No.		Scalable to add new device, grid / sub-station, network, subnet, without any change in dbase and storage.	Any change to any device such as communication change, asset change, vulnerability change, etc., is captured within the database and will therefore require result in a change to the backend database. (Threat Intel / Asset Intel)	Clause is clear
32	6.2		Hotfix / patch / upgrade to Operating system, (provided by OEM) of hosting environment for next 5 yrs	Does this mean the provided IDS solution patching ? Since IDS does not automatically patch or block anything.	It contains all devices which is provided as part of the project including hardware and software

Corrigendum 1

IMPLEMENTATION OF OT SECURITY ''REAL THREAT & VULNERABILITY MANAGEMENT SYSTEM" IN BYPL
NIT NO: CMC/BY/24-25/RS/SkS/APT/51
[RFx Number: 2200000084]

Calrifications to the per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
33	7.4		Termination for default	We propose to add the new clause as per below: In the event Purchaser materially breaches this Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the Purchaser, the Supplier may terminate this Agreement or any portion thereof or the applicable statement of work by giving written notice to the Purchaser.	Tender condition shall prevail.
34	55		Non-solicitation	We propose to add the new clause as per below: During the Term (including renewal term, if any) of the Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been engaged to provide/perform the Services) of the other Party or aid any third person to do so, without the specific written consent of the other Party. This provision shall however not apply to any solicitation conducted through general advertisement of employment opportunities through placement agencies, public advertisement or otherwise which do not specifically target such employees. The said restriction shall also applies to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, "Representatives"). Parties agree that representatives are equally prohibited from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party.	Tender condition shall prevail.
35			Terms of Payment and Billing : For Supply of Equipment's (Part-A):	We propose for MS-1: 70% of contact value for of Pricing schedule shall be released subject to fulfillment on Delivery of required hardware and licenses, since installation is mention on MS-2: 20% of contact value itself.	Tender condition shall prevail.
37	Page No-6; Section:2.01 Technical Criteria; Clause No-2		a. Purchase Order copies b. Performance Certificate/ Completion certificate/ Invoice Copies If bidder is an authorized partner of OEM, credentials/ Declaration of OEM shall also be considered against this QR	We have Non-disclosure agreement signed with our customers, hence we request you to kindly accept the maksed PO and declaration as document against past experience.	Tender condition shall prevail.
39	Page No-6; Section:2.01 Technical Criteria; Clause No-3		a) Thee reference PO copies to be provided. b) Bidder to share one PO details having reference of 15 sites or 1000 asset license. c) Certificate copies of resources to be deployed for implementation and support.	We have Non-disclosure agreement signed with our customers, hence we request you to kindly accept the maksed PO and declaration as document against past experience.	Tender condition shall prevail.
40	2.01 Technical Criteria, Point 2	6	The Bidder must have completed minimum three (03) similar full cycle implementation of offered OT security systems in the last five (05) years prior to the date of bid submission of which at least one (01) implementation should be in Power/ Energy/Utility sector.	Kindly change this clause to bidder/OEM i.e. The Bidder/ OEM must have completed minimum three (03) similar full cycle implementation of offered OT security systems in the last five (05) years prior to the date of bid submission of which at least one (01) implementation should be in Power/ Energy/ Utility sector.	No change in the RFP clause
41	2.01 Technical Criteria, Point 3	6	The Bidder should have minimum Five (5) years' experience in providing at least 03 supply, implementation and technical support services for OT deployment engagements in Govt sector, power sector, energy, BFSI or critical sector	Kindly change this clause to bidder/OEM i.e. The Bidder/ OEM should have minimum Five (5) years' experience in providing at least 03 supply, implementation and technical support services for OT deployment engagements in Govt sector, power sector, energy, BFSI or critical sector	No change in the RFP Clause
42	VOLUME – III TECHNICAL SPECIFICATIONS, Point No.6.2	74	Scalable to add new device, grid / sub-station, network, subnet, without any change in dbase and storage	Kindly remove this point as Any change to any device such as communication change, asset change, vulnerability change, etc., is captured within the database and will therefore require result in a change to the backend database.	No changhe in the RFP clause We are refereing to the scalability of the offered system. Central system provided should capable to support atleast 90 sites without any upgradation in hardware from day one.

Corrigendum 1

IMPLEMENTATION OF OT SECURITY ‘’REAL THREAT & VULNERABILITY MANAGEMENT SYSTEM” IN BYPL
NIT NO: CMC/BY/24-25/RS/SkS/APT/51
[RFx Number: 2200000084]

Calrifications to the per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
43	1. SCOPE OF WORK	76	c) Implementation: Bidders require to provide the POC as per the BYPL request and requirement before finalization of the system. BYPL reserve the rights to qualify or disqualify bidder solution based on PoC out come and deliverables. OEM product who has successfully completed PoC of bid product in BSES Rajdhani Power Ltd or BSES Yamuna Power Ltd, with 100% discovery of IP connected devices (IP, Mac) and at least 80% visibility of connected devices (make, model, firmware) for a given location, can only be taken for commercial opening of bid document.	Please confirm whether an OEM that has successfully completed a PoC in BSES Rajdhani or BSES Yamuna Power Ltd will have the prior PoC considered valid, or if a new PoC is required for this specific bid ?	Yes, Prior PoC will be valid but BYPL reserve rights to perform PoC again.
44	1. SCOPE OF WORK	77	i) Software and Firmware Licenses: Bidder shall ensure that all System Software Licenses offered shall be purchased under the name of purchaser (BYPL). For this project, the Licenses shall be Enterprise wide full use, perpetual without any restriction on access/usage of any kind of functionality during the Guarantee/ maintenance support period, post completion of contract and handover all Software Licenses (latest version deployed) to purchaser.	Some of the OEM licenses for the offered solution are subscription-based rather than perpetual licenses. In this case, could you please clarify the required duration for the subscription license? Should it be for a 3-year or 5-year period?	It is for a period of 5 years from the date of Go-live of the project.
45		77	h) Training: Bidder must provide training periodic sessions on product use to BYPL team for efficient, viable and fully functional system.	As per our understanding, the bidder will provide the initial user and admin training to kick-start the operation of the entire system. This training will consist of a maximum of 2 batches, with 10 trainees in each batch. If this is not the case, kindly provide answers to the following queries: 1. How often are the periodic training sessions expected to occur (e.g., monthly, quarterly, etc.), and how many batches and trainees will be included in each session? 2. What is the expected duration for each training session? 3. Is there a preferred mode of delivery for the training sessions (Onsite, Remote)?	Admin and user level training to BYPL staff needs to be provided by OEM and Bidder at the time of kick-start and go-live. Halfyearly brush up training needs to be conduted inculding along any new features introcuce in the system. Training should be Onsite.
46	3. Architecture (IT & OT):	78	d) Solution should be appliance-based product which includes both hardware and software.	As per our understanding, you need a solution with integrated hardware and software, which means we can consider either an appliance-based solution or a VM-based solution that can be hosted on any embedded hardware. Please confirm if our understanding is correct.	Site sensors or devices should be industrial grade hardened appliance based device only. No server VM based solutions. At central datacenter harden appliance or VM based solution can be accepctable. Sensors for site locations should have DC power input. Sensors for site should have atleast 3 x1G (copper) traffic capture/ monitoring ports and one management port.
47	3. Architecture (IT & OT):	78	e) System installed (Hardware and Software) at central should be in HA mode	As per our understanding, you require high availability only for the management console, which will provide top-level monitoring of all IDS sensors and IDS appliance at thesubstation and control centre. Please confirm if our understanding is correct.	All solution deployed at central datacenter should be in HA. Naming termonology can be different for OEM's.
48		78	Phase 4 - Deploy the solution at each site as per site readiness and obtain signoff. Deliver and install the solution at respective sites as per the approved design Configure the solution and establish connectivity between Site OT Server and sensors Deploy the data diode at respective sites for integration with business network.	As per our understanding, the customer will provide the DATA Diode along with all required licenses for the number of tags. The bidder is only required to include the integration effort in the proposal. Please confirm if our understanding is correct.	Yes, Data diode is not part of the supply.
49	4. IMPLEMENTATION APPROACH	79	Phase 6 - Integrate the solution with / SIEM / ITSM / SOAR solution Integrate OT Management server with SIEM / ITSM / SOAR solution through data diode solution Perform pilot monitoring for one week before go live.	Could you please provide more information regarding the specific SIEM or SOAR system with which you want to integrate the OT Management server? This will help us assess the compatibility with our proposed solution.	All major OEM's of SIEM SOAR like but not limited to Logrhythm, IBM Qradar, Microfocus, Splunk, Innspark, Paloalto, Fortigate etc

Corrigendum 1

IMPLEMENTATION OF OT SECURITY ''REAL THREAT & VULNERABILITY MANAGEMENT SYSTEM" IN BYPL
NIT NO: CMC/BY/24-25/RS/SkS/APT/51
[RFx Number: 2200000084]

Calrifications to the per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
50	4. IMPLEMENTATION APPROACH	79	Phase 6 - Integrate the solution with / SIEM / ITSM / SOAR solution Integrate OT Management server with SIEM / ITSM / SOAR solution through data diode solution Perform pilot monitoring for one week before go live.	As per our understanding, bidders will only provide man-hour support for integrating the OT Management server with the existing SIEM through a Data Diode. All required licenses or subscriptions for the Data Diode, SIEM, or SOAR will be provided by BSES. Please confirm if our understanding is correct.	Yes, All licenses of SIEM SOAR Data diode will be provided by BYPL.
51		79	Phase 7- Declare go live of respective site and initiate monitoring the alerts. Bidder shall deploy required manpower. Provide knowledge transfer / training session to the Site SPOC Provide access of the solution to the Site team and provide them training. Operationalize the site and initiate 24x7 monitoring. Perform 24x7 monitoring of the OT Server. Report alerts to the respective Site Team providing details of the alert. Close the alert based on the response from the Site team. Steady state enhancement for enrichment & continual improvement. Provide weekly and monthly operations report.	As per our understanding, you require site engineers only at the central location to monitor and manage all assets distributed across 65 sites. 1. Could you please clarify the number of resources required at central site for monitoring? The RFP specifies 24*7 monitoring, and on page 82, paragraph 13, under the "Scope of Work - Operation" section, it is mentioned that 2 resources (L1) are required for 8-hour shifts. 2. Could you please clarify whether you require a resident engineer for 24*7 operation, or if the engineers will be supporting the customer site team remotely?	Engineer require for on site monitoring and support. 2 onsite resources (L1) are required in 8-hour shift. Shift timming will be finalize after finilazation of the parther.
52	13. Scope of Work: Operations	82	Provide resources 2 Nos, L1 in 8 hr. shift. Resource should be certified on the offered and deployed solution.		Prefered to be certified on the offered soultion
53	7. Secure Design & Access:	80	a. Authorization & Authentication: i. Supports multi-factor authentication for admin activities ii. Least privilege System, allow granular permission levels, to assets and Sites, access times for each user or group, user and group permissions for file transfers and file access etc.	As per our understanding, bidders will only provide man-hour support for integrating the OT users with the existing MFA solution. All required licenses or subscriptions for adding OT users will be provided by BSES. Please confirm if our understanding is correct.	Yes, Understanding is correct
54	12. Project Completion & Sign-Off		h. For all hardware – Submission of valid Certificate of common criteria as per IEC / ISO 15408, issued by CPRI lab.	CPRI does not provide certification for Common Criteria (ISO/IEC 15408) and is primarily focused on testing, certification, and research in accordance with IEC standards related to the electrical power sector (OT devices only). Please remove this requirement from the specification as it is not applicable, as CPRI does not provide certification for IT products, and the product we are proposing falls under the category of IT products.	This clause is applicable only if the product falls under the said category of common criteria as per IEC / ISO 15408.
55	11. Deployment & Training:	81	b. Grid will be said complete, only when it's all connected assets are visible in solution, baseline established, alerts & reports are configured, with user acceptance.	As per our understanding, all connected assets refer to the assets that have an IP address and must be visible within the solution. Please confirm.	Yes, all IP assets
56	Award Decision	Pg 10, point 4.05	Rate shall remain FIRM till the validity of the Contract.	USD fluctuation and OEM upflift to be acceomodated by BSES	Tender condition shall prevail.
57	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.	The Referred PBGs are same.
58	Indemnification, Pg 55	Pg 55, point 33	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.
59	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.	Tender condition shall prevail.
60	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.	Tender condition shall prevail.

Corrigendum 1

IMPLEMENTATION OF OT SECURITY ‘’REAL THREAT & VULNERABILITY MANAGEMENT SYSTEM” IN BYPL
NIT NO: CMC/BY/24-25/RS/SkS/APT/51
[RFx Number: 2200000084]

Calrifications to the per-bid queries

S.No.	NIT Section Name & No	NIT Page No	NIT Clause Descriptions	Clarifications / Suggestions Required by Bidders	BSES Response/ Clarification
61	Earnest Money Deposit (EMD)		6,75,000/- (Rupees Six Lakh and Seventy Five Thousand)	As per the Public Procurement Policy for Micro and Small enterprises order 2012,The Registered MSEs are exempted from tender fees and EMD. Request to provide the Exemptipn of Tender fee and EMD for MSE bidders.	Tender condition shall prevail.
62	Technical Criteria		The Bidder should have minimum Five (5) years’ experience in providing at least 03 supply, implementation and technical support services for OT deployment engagements in Govt sector, power sector, energy, BFSI or critical sector	Request to consider the PO copies from Ong, Pharma and Manufacturing sector as well.	No change in the RFP clause. Read along with document to be submitted
63	Technical Criteria		The Bidder should have minimum Five (5) years’ experience in providing at least 03 supply, implementation and technical support services for OT deployment engagements in Govt sector, power sector, energy, BFSI or critical sector	Please confirm- Out of 3 PO Only One PO older than 5 years can be submitted to qualify in this clause.	Yes, Understanding is correct
64	Technical Compliance Clause no 3.2		For each CVE, active threat intelligence shall be provided indicating following at a minimum: a. Exploit Code Maturity, b. Vulnerability Age & Product Coverage, c. Threat Intensity By Malicious Actors, d. Threat Activity Regency, And Sources Of Threat Information	We request to amend this clause as below- "For each CVE, the solution provided should have threat intelligence in the form of Advisories from CISA/OEM which gives globally published details on Exploit Code information, Vulnerability age & Product Coverage, Mitigation, Threat Severity, etc. The solution should bring the characterization of Threat in the form of CISA-KEV(Known Exploited Vulnerabilities), EPSS, Exploit DB, etc."	No change in the RFP clause
65	Technical Compliance Clause no 5.3		Able to take Backup of sys logs for min 180 days. Capable to restore system configuration.	Request to amend this clause as below- "Solution should be able to store insights and Threat Alerts locally in the platform for 180 days"	All logs of the offered system should be stored centrally for atleast 180 days as per Govt. guidelines. Storage needs to be planned accordingly at dat center.
66	Technical Compliance Clause no 7.1		MITRE Attack, NIST, IEC 62443, NCIIPC, NIST-CRP etc	Please share us the list of IDS points related to NCIIPC framework for us to validate. What all points related to OT Cyber security to be qualified from NCIIPC?	Please check various orders like (not limited to): **a.** Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 **b.** Objective of Cyber Security Guidelines issued by MoP/CEA in Oct2021.
67	Technical Compliance Clause no 7.2		Encryption level and server hardening certificate	Request to remove the Server hardening certificate. Claroty can provide a documentation with the details of Encryption level used in Data in Transit and Rest.	Details of encryption and server hardening needs to be provided
68	SOW		Logs: Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc. Additionally, the access to such logs must be controlled in accordance to the least-privilege concept mentioned above, so that entries may not be deleted, accidentally or maliciously	Request to share the additional details on this clause.	Clause is well explanotary.
69	SLA	82	SLA	The SLA and penalty has been provided for response and resolution time for the solution. Since there is no requirement of 24x7 onsite team, the response and resolution time will be difficult to achieve. As such there can be a SLA for 95% uptime of the solution which the bidder has to provide and accordingly the penalty clause may be revised.	This is w.r.t warranty and support of copmplete solution which will be handled by support team of Bidder/OEM which will be separate form operations team.
70	Scope of work for Operations	82	Scope of work for Operations	Please provide details and elaborate the roles and activities to be performed by the Shift team	Operations team is responsible (not limited to) to manage all alerts and fine tunning of the system including identifying false positive and true positive. This team needs to work in close cordination with SOC and BYPL OT team. Reporting to BYPL team on any anomaly identifiy in the system.