Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
1	Section II; Clause 2.5; Sl. No. 6; Page No. 8	Last Date and Time for Submission of e-Bid	During the period of 24th December to 8th January most organizations, especially international OEMs, would be operating on a limited scale due to the holiday season. So we would request DIT, Govt. of Tripura to kindly extend the bid submission deadline to a date beyond 11th January 2023.	Refer corrigendum dated 28.12.2022
2	Section III; Clause 1; Sl. No. 1; Page No. 11	The Bidder shall submit Earnest Money Deposit (EMD) of Rs.10,00,000/- (Rupees Ten Lakh only) through online in the https://tripuratenders.gov.in portal.	The Bidder shall submit Earnest Money Deposit (EMD) of Rs.10,00,000/- (Rupees Ten Lakh only) through online in the https://tripuratenders.gov.in portal or in the form of BG from any scheduled bank.	No change.
3	Section III; Clause 3; Sl. No. 1; Page No. 11	The Bidder shall submit Earnest Money Deposit (EMD) of Rs.10,00,000/- (Rupees Ten Lakh only) through online in the https://tripuratenders.gov.in portal.	We would request DIT, Govt. of Tripura to kindly accept the EMD as a Bank Guarantee which is a standard widely accepted instrument for accepting EMD.	No change.
4	Section III; Clause 3; Sl. No. 2; Page No. 11	The Bidder should be registered under the Companies Act, 1956 or Companies Act 2013, and should have been in existence for the last 3 (three) years from the date of publishing the RFP.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company incorporated under Companies Act, 2013 as a wholly owned subsidiary of the main Parent Company. In view of the above we would request DIT, Govt. of Tripura to kindly consider the relevant documentary evidence of both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance. Please confirm the acceptance of our request.	Please submit relevant documents for consideration.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
5	Section III; Clause 3; Sl. No. 3; Page No. 11	The Bidder shall have an average annual turnover of INR 20.00 crore and positive networth in each of the last three (3) financial years ended on 31/03/2021.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request DIT, Govt. of Tripura to kindly consider the audited financial statements of both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance. Please confirm the acceptance of our request.	Please submit relevant documents for consideration.
6	Section III; Clause 3; Sl. No. 4; Page No. 11	Bidder's experience of having successfully completed Data Center (DC) / Security Operation Center (SOC) setup work: a) for State/ Central Govt. Agencies or PSUs or PSU Banks or Financial Institutions of State/Central Govt. of India will be considered. b) Single Project of an order value not less than Rs.5.00 crore or Two Projects of order values not less than Rs.4.00 crore for each projects or Three or more Projects of order value not less than Rs.3.00 crore for each projects will be considered during the period from 1st April 2016 to previous day of floating of the tender. c) Cost of civil works for DC/SOC won't be considered for calculating cost in this purpose.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request DIT, Govt. of Tripura to kindly consider the documentary evidence of the relevant projects delivered by both the Parent Company and the Subsidiary Company (Bidder) for RFP compliance. Please confirm the acceptance of our request.	Please submit relevant documents for consideration.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
7	Section III; Clause 3; Sl. No. 4; Page No. 11	Bidder's experience of having successfully completed Data Center (DC) / Security Operation Center (SOC) setup work: a) for State/ Central Govt. Agencies or PSUs or PSU Banks or Financial Institutions of State/Central Govt. of India will be considered. b) Single Project of an order value not less than Rs.5.00 crore or Two Projects of order values not less than Rs.4.00 crore for each projects or Three or more Projects of order value not less than Rs.3.00 crore for each projects will be considered during the period from 1st April 2016 to previous day of floating of the tender. c) Cost of civil works for DC/SOC won't be considered for calculating cost in this purpose.	Bidder's experience of having successfully completed Data Center (DC - Compute / Storage / Network etc. activity)/ Security Operation Center (SOC) setup work: a) for State/ Central Govt. Agencies or PSUs or PSU Banks or Financial Institutions of State/Central Govt. of India will be considered. b) Single Project of an order value not less than Rs.5.00 crore or Two Projects of order values not less than Rs.4.00 crore for each projects or Three or more Projects of order value not less than Rs.3.00 crore for each projects will be considered during the period from 1st April 2016 to previous day of floating of the tender. c) Cost of civil works for DC/SOC won't be considered for calculating cost in this purpose.	Please refer corrigendum.
8	Section IV; Clause 4.1; Sl. No. 2; Page No. 13	Bidder should provide complete services which includes installation/implementation, integration, management, maintenance, support, audit compliance and knowledge transfer	How CSOC Bidder can provide audit compliance. its the responsibility of 3rd parties. As it's a contradictory requirement hence requesting tendering authority to Remove this point from Bidder Scope.	Please refer corrigendum.
9	Section IV; Clause 4.1; Sl. No. 4; Page No. 13	The solution should provide centralized management console for Anti-DDOS & WAF appliances. Which will cover analytics dashboards, performance statistics and reporting functionalities	1. This centralized management console for Anti-DDOS & WAF appliances is part of BOQ ? Also this can restrict multiple OEM participation. 2. Please calrify what do you mean analytics dashboards, any use-case.	Please refer corrigendum.
10	Section IV; Clause 4.1; Sl. No. 10; Page No. 13	The replacement of parts, if any, during the entire period of contract will have to be provided by the OEM and should be new. Refurbished parts should not be supplied as replacement.	Kindly confirm this applies to the solution components proposed as part of RFP scope and not for peripheral, supporting infra of SDC.	Please refer corrigendum.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
11	Section IV; Clause 4.1; Sl. No. 12; Page No. 13	The successful bidder shall provide on-site training to designated person(s) nominated by DIT-TSDC on administration & usage features of the supplied solution within 30 days of the successful installation in TSDC	Kindly confirm the expected batch size of trainees and duration of on-site training to be conducted.	Please refer corrigendum.
12	Section IV; Clause 4.1; Sl. No. 14; Page No. 13	Should be able to integrate with all devices irrespective of the OEM or manufacturer.	We would request DIT, Govt. of Tripura to kindly share the complete details (make / model / version / release) of the existing devices which needs to be integrated.	Would be shared with selected bidder only.
13	Section IV; Clause 4.1; Sl. No. 14; Page No. 13	Should be able to integrate with all devices irrespective of the OEM or manufacturer.	Please share the List of Expected devices to be integrated. Also, certain Legacy Devices need to be excluded from the devices list. Reason integration feasibility and non-supported sources.	Would be shared with selected bidder only.
14	Section IV; Clause 4.2.1; Sl. No. (a); Page No. 14	The Bidder shall setup an onsite SOC at the TSDC premises and provide the required security services for period of 3 years	Here DIT asking to setup Onsite SOC at the TSDC premises But if Bidder has to provide the SOC. Please share the BOQ for SOC Setup Specification is not metioned like; 1. Dimention of the SOC Room 2. VideoWall Monotor Size, 3. L1 and L2 Workstation specification 4. Interior Setup(Flooring, false Ceiling, AC, light and furnitur) 5. Server Racks 6. uninterruptible power supply (UPS)	Please refer corrigendum.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
15	Section IV; Clause 4.2.1; Sl. No. (b); Page No. 14	The onsite resources (People, Process and Technology) required to run and manage the SOC shall be deployed from the bidder's own sources to manage, monitor, analyze, mitigate, and report incidents as they occur alongwith onsite monitoring.	We understand that DIT, Govt. of Tripura would provide the necessary office setup such as furnished space, AC, power & UPS facility, internet connectivity, telephone (landline), access to common facilities etc. for the onsite resources. Please confirm our understanding.	Please refer corrigendum.
16	Section IV; Clause 4.2.2; Sl. No. (b); Page No. 14	Identification and Prevention of Information Security Vulnerabilities: The SOC should be able to identify information security vulnerabilities in the SDC's environment and prevent these vulnerabilities through implementation of adequate security solutions	As security vulnerabilities can be on the assets not managed by the SOC team in that case prevention is the responsibility of the asset custodian/owner. Secondly implementation of any other security solution deemed as adequate at any specific time during operations not mentioned in this RFP is out of scope. Thus request you to modify this statement as "*Identification and Prevention of Information Security Vulnerabilities: The SOC should be able to identify information security vulnerabilities in the SDC's environment and help SDC to mitigate them.* "	Please refer corrigendum.
17	Section IV; Clause 4.2.3; Sl. No. (a); Page No. 15	Minimum Qualification, Relevant Experience & Certification	We would request DIT, Govt. of Tripura to kindly review the minimum qualification & certification requirement since hiring and deploying technical resources having high-end skillset at Agartala has multiple practical challenges. We would suggest the following as a possible alternative: SOC Level 2 Analyst: BE / B. Tech. / MCA / MSc. / MBA with 4 years of relevant experience SOC Level 1 Analyst: BE / B. Tech. / MCA / MSc. / MBA with 1 year of relevant experience	No change.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
18	Section IV; Clause 4.2.3; Sl. No. (b); Point No. 2; Page No. 14	...Perform additional auxiliary responsibilities as when required.	For resource factoring, please list the additional auxiliary responsibilities as and when required.	No change.
19	Section IV; Clause 4.2.1; Sl. No. (i); Page No. 14	There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on DIT. The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required.	We would request DIT, Govt. of Tripura to kindly share the complete details (make / model / version / release) of the existing devices which needs to be integrated. The proposed solution would address all the devices that are listed by DIT, Govt. of Tripura in this RFP document. However in case new devices / technologies are introduced during the contract period then the necessary licenses & implementation cost would be applicable. Please confirm the acceptance of our request to align with the industry wide accepted standard protocol for similar projects.	Would be shared with selected bidder only.
20	Section IV; Clause 4.2.1; Sl. No. (b); Page No. 14	The onsite resources (People, Process and Technology) required to run and manage the SOC shall be deployed from the bidder’s own sources to manage, monitor, analyze, mitigate, and report incidents as they occur alongwith onsite monitoring.	Please specify what operations hours for Onsite monitoring is required. Our Suggestion: Generally for any SOC environments prefer 24/7x365 monitoring either completely onsite or in Hybrid-Mode (e.g. 8hrs onsire and rest 16hrs Offsite)	10:00 am to 6:00 pm in all working days.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
21	Section IV; Clause 4.2.1; Sl. No. (c); Page No. 14	All the proposed items to be deployed in TSDC premises	Does the bidder need to deploy the required solution with HA (High Availability) support? If Yes, Please clarify 1. Server Security Solution 2. WAF 3. DDoS Mitigation Solution 4. SIEM 5. SOAR 6. Anti-APT 7. VA Tool	HA not asked for.
22	Section IV; Clause 4.2.1; Sl. No. (c); Page No. 14	All the proposed items to be deployed in TSDC premises	We request you to please consider SaaS based solution hosted in India which is Meity approved for Web application VA tool, as the public facing applications needs to be scanned from external personna as well.	Please refer corrigendum.
23	Section IV; Clause 4.2; Page No. 14	Additional Query on IT Security Infrastructure for Tripura Security Operation Center (SOC)	Some of the components to be delivered as part of RFP scope are Virtual Security tools. Kindly confirm if the underlying infrastructure, compute, network etc. for deploying the same will be provided by SDC or bidder has to account for it.	Please refer corrigendum.
24	Section IV; Clause 4.2.3; Sl. No. (a); Page No. 15	SOC Level 2 Analyst SOC Level 1 Analyst	Perceiving the financial benefit of the organization i.e., DIT-Tripura. Keeping an Onsite SOC Level 2 certified personal will unnecessarily increase the budget. Hence requesting tendering authority to modify this clause as SOC Level 1 Analyst resources onsite and L2/L3 monitoring from the bidder's own SOC 2 Type II certified SOC	No change.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
25	Section IV; Clause 4.2.3; Sl. No. (d); Point No. 2; Page No. 16	After deputing the selected resources, the selected bidder shall replace immediately any of its manpower who is found unacceptable because of under-performance/ security risks/ incompetence/ conflict of interest/ improper conduct etc. upon receiving a notice from DIT. Manpower could be canceled with 30 days notice period for knowledge transfer. New replacement of the manpower should be made available before 7 days of notice period of canceled manpower is over.	We would request DIT, Govt. of Tripura to kindly appreciate the fact that hiring & deploying technical resources with niche skillsets is difficult. So we would request DIT to kindly amend the clause as suggested below: *Manpower could be cancelled with 90 days notice period for knowledge transfer. New replacement of the manpower should be made available before 7 days of notice period of cancelled manpower is over.*	No change.
26	Section IV; Clause 4.2.3; Sl. No. (d); Point No. 3; Page No. 16	If any manpower provided by the selected bidder intends to resign then he/she should serve 30 days notice period. Agency must ensure that new replacement of the manpower should be made available immediately after when notice period of resigned manpower finished.	We would request DIT, Govt. of Tripura to kindly appreciate the fact that hiring & deploying technical resources with niche skillsets is difficult. So we would request DIT to kindly amend the clause as suggested below: *If any manpower provided by the selected bidder intends to resign then he/she should serve 90 days notice period. Agency must ensure that new replacement of the manpower should be made available immediately after when notice period of resigned manpower finished.*	No change.
27	Section IV; Clause 4.2.3; Sl. No. (d); Point No. 4; Page No. 16	The employee deployed under the contract shall be entitled to 12 (twelve) Casual Leave (CL) in a calendar year. If employee joins middle of the year then eligible CL will be on pro-rata basis.	We would request DIT, Govt. of Tripura to kindly amend the clause as suggested below to accommodate Earned Leaves (EC) of the resource: *The employee deployed under the contract shall be entitled to 12 (twelve) Casual Leave (CL) and 15 (fifteen) Earned Leave in a calendar year. If employee joins middle of the year then eligible CL will be on prorata basis. 15 EL is accumulated by a confirmed resource for every year of continued service.* Please confirm the acceptance of our request to align with the industry wide accepted standard HR policy.	No change.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
28	Section V; Clause 5; Sl. No. 19; Page No. 18	Any other item	1. Please confirm if we need to propose the underlying IT infrastructure which would be required for implementing the security solutions such as servers, storage, OS licenses, DB licenses etc. 2. Please share the IT and Non-IT infra such as UPS, racks, cabling, VMs, licenses etc. that DIT, Govt. of Tripura would provide for implementing the required security solution.	Please refer corrigendum.
29	Section VI; Clause 6.1; Page No. 22	Period of Validity of Bids shall remain valid for 270 days after the date of opening of Bids prescribed by the DIT.	Requesting tendering authority to modify this and reduced to 180 days	No change.
30	Section VII; Clause 7.3; Sl. No. 4; Page No. 27	Support/ Maintenance: OPEX will be paid quarterly after completion of each quarter period and submission of bill (during support period of 3 years) as per financial bid of selected bidder.	We would request DIT to kindly process the payment for AMC / ATS of the supplied solution on an annually in advance basis so as to along with the payment schedule of the OEMs.	No change.
31	Section VII; Clause 7.3; Page No. 27	**Payment Terms & Schedule:** 1. Delivery: 70% of total CAPEX value after delivery of all items ordered.	Requesting tendering authority to modify as *70% of respective solution on delivery of the same.*	No change.
32	Section VII; Clause 7.3; Page No. 27	**Payment Terms & Schedule:** 2. Installation and Successful FAT: 30% of total CAPEX value after successful installation, commissioning & submission of Final Acceptance Certificate.	Requesting tendering authority to modify as *30% of respective solution on installation, commissioning & submission of FAT* .	No change.
33	Section VII; Clause 7.3; Page No. 27	**Payment Terms & Schedule:** 3. Support/ Maintenance: OPEX will be paid quarterly after completion of each quarter period and submission of bill (during support period of 3 years) as per financial bid of selected bidder.	Requesting tendering authority to modify as *To be paid Quarterly in Advance as OEM takes the entire support along with the product/software.*	No change.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
34	Section VII; Clause 7.4; Sl. No. 1 & 2; Page No. 27	1. Supply of all the equipment should be within 12 weeks after the allotment of work order from DIT. 2. Installation, configuration and commissioning of the IT Security Infrastructure need to be completed within 16 weeks of work order issue date.	Due to the prevalent shortage of microprocessor chips, ongoing COVID-19 related severe restrictions in China wherein majority of the chip manufacturers are located and the ongoing Russia – Ukraine conflict there is a global slowdown in the supply chain of IT equipment. Hence, we would request DIT, Govt. of Tripura to kindly extend the delivery timeline as suggested below: 1. Supply of all the equipment should be within 24 weeks after the allotment of work order from DIT. 2. Installation, configuration and commissioning of the IT Security Infrastructure need to be completed within 10 weeks from the date of delivery of ordered hardware and software licenses.	No change.
35	Section VII; Clause 7.4; Sl. No. 1; Page No. 27	1. Supply of all the equipment should be within 12 weeks after the allotment of work order from DIT.	Requesting tendering authority to modify as Delivery: 24 weeks	No change.
36	Section VII; Clause 7.4; Sl. No. 2; Page No. 27	2. Installation, configuration and commissioning of the IT Security Infrastructure need to be completed within 16 weeks of work order issue date.	Requesting tendering authority to change the Installation, configuration and commissioning as below: Milestone based implementation: WAF: 8 Weeks from hardware/lic delivery. DDOS: 8 Weeks from hardware/lic delivery. Server Security: 12 weeks from hardware/lic delivery Anti APT: 16 weeks from hardware/lic delivery VA Tool: 18 weeks from hardware/lic delivery Intel feeds: 22 weeks from hardware/lic delivery SIEM: 24 weeks from hardware/lic delivery SOAR: 28 Weeks from hardware/lic delivery	No change.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response

37	Section VII; Clause 7.5; Sl. No. 1 (Table); Page No. 28	Up to 1 week - 1% of the CAPEX amount;
		Up to 2 weeks - 2% of the CAPEX amount;
		Up to 3 weeks - 3% of the CAPEX amount and so on;
		Up to 5 weeks - 5% of the CAPEX as maximum penalty;
			We would request DIT, Govt. of Tripura to kindly amend the penalty charges as suggested below:
			
			Up to 1 week - 1% of the cost of the undelivered items;
			Up to 2 weeks - 2% of the cost of the undelivered items;
			Up to 3 weeks - 3% of the cost of the undelivered items and so on;
			Up to 5 weeks - 5% of the cost of the undelivered items as maximum penalty;
				No change.

38	Section VII; Clause 7.5; Sl. No. 1 (Table); Page No. 28	**Penalty for delivery:**
		Up to 1 week - 1% of the CAPEX amount;
		Up to 2 weeks - 2% of the CAPEX amount;
		Up to 3 weeks - 3% of the CAPEX amount and so on;
		Up to 5 weeks - 5% of the CAPEX as maximum penalty;
			Requesting tendering authority to modify as
			to define is solution specific rather than the entire Capex as multiple OEM involvement.
				No change.

39	Section VII; Clause 7.5; Sl. No. 2; Page No. 28	Installation of all components, integration, Final Acceptance Test (FAT) and Go-Live: Within 16 weeks of work order issue date - A Penalty of 0.25% of CAPEX for every week or part thereof delay upto 6 weeks delay. Beyond 6 weeks, penalty would be 0.5% of CAPEX for every week or part thereof.	We would request DIT, Govt. of Tripura to kindly cap the total penalty charges at a maximum value of 10% of the CAPEX.	No change.
40	Section VII; Clause 7.5; Sl. No. 3; Page No. 28	**Service levels for onsite required Resources:** Any replacement of onsite manpower resource need to complete in zero (0) day gap, else DIT will deduct wages for non-deployed manpower resources in the onsite DCO team and DIT will deduct penalty as per following rate: SOC Level 1 Analyst: 2% of Monthly wages per person per working day SOC Level 2 Analyst: 2% of Monthly wages per person per working day.	We would request DIT, Govt. of Tripura to kindly amend the penalty charges as suggested below: Service levels for onsite required Resources: Any replacement of onsite manpower resource need to complete in 7 days gap, else DIT will deduct wages for non-deployed manpower resources in the onsite DCO team and DIT will deduct penalty as per following rate: SOC Level 1 Analyst: 1% of Monthly wages per person per working day SOC Level 2 Analyst: 1% of Monthly wages per person per working day	No change.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
41	Section IX; Clause 9.2; Sl. No. 1; Page No. 37	The Bidder should be registered under the Companies Act, 1956 or Companies Act 2013, and should have been in existence for the last 3 (three) years from the date of publishing the RFP.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company incorporated under Companies Act, 2013 as a wholly owned subsidiary of the main Parent Company. In view of the above we would request DIT, Govt. of Tripura to kindly consider the relevant documentary evidence of both the Parent Company and the Subsidiary Company (Bidder) for Technical Evaluation Criteria compliance & scoring. Please confirm the acceptance of our request.	Please submit relevant documents for consideration.
42	Section IX; Clause 9.2; Sl. No. 2; Page No. 37	The Bidder shall have an average annual turnover of INR 20.00 crore and positive networth in each of the last three (3) financial years ended on 31/03/2021.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request DIT, Govt. of Tripura to kindly consider the audited financial statements of both the Parent Company and the Subsidiary Company (Bidder) for Technical Evaluation Criteria compliance & scoring. Please confirm the acceptance of our request.	Please submit relevant documents for consideration.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
43	Section IX; Clause 9.2; Sl. No. 3; Page No. 37	Bidder's experience of having successfully completed Data Center (DC) / Security Operation Center (SOC) setup work: a) for State/ Central Govt. Agencies or PSUs or PSU Banks or Financial Institutions of State/Central Govt. of India will be considered. b) Single Project of an order value not less than Rs.5.00 crore or Two Projects of order values not less than Rs.4.00 crore for each projects or Three or more Projects of order value not less than Rs.3.00 crore for each projects will be considered during the period from 1st April 2016 to previous day of floating of the tender. c) Cost of civil works for DC/SOC won't be considered for calculating cost in this purpose.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request DIT, Govt. of Tripura to kindly consider the documentary evidence of the relevant projects delivered by both the Parent Company and the Subsidiary Company (Bidder) for Technical Evaluation Criteria compliance & scoring. Please confirm the acceptance of our request.	Please submit relevant documents for consideration.

44	Section IX; Clause 9.2; Sl. No. 3; Page No. 37	**Point System:**
		Single project unit = 14 marks;
		2 project units= 16 marks; 3 project units=18 marks;
		4 or more project units=20 marks;
			We request you to kindly refer below changes for better and healthy participation:
			Point System:
			Single Project order value 5 cr to 6 cr = 14 marks;
			Single Project order value 7 cr to 8 cr= 17 marks;
			Single Project order value 9 cr to 10 cr=20 marks;
				No change.

45	Section IX; Clause 9.2; Sl. No. 3; Page No. 37	Work Order + Completion/ Phase Completion Certificates from the client; 4 or more project units=20 marks;	Please clarify whether do bidder need to provide the experience of all the solution mentioned in your RFP for each project of a minimum 4 Nos.?	Clause is self-explanatory.
46	Section X; Clause 10; Sl. No. 2 & 3; Page No. 42	2. The value of CAPEX should not be more than 75% of the total project value. 3. Items listed at serial 1 to 8 in BoM section of this RFP would be considered as CAPEX items and Items listed at serial 9 to 18 in BoM section of this RFP would be considered as OPEX items.	Please remove this clause.	No change.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
47	Additional Query	NA	Please share the current count of Web applications required to prepare the BOQ of Web Application VA tool.	Please refer corrigendum.
48	Additional Query	NA	If any ticketing tools is currently being utilized then please share its details (like product name, version, license etc.) so that bidder could look for scope of utilizing the same for tickets related to security incidents.	There is no ticketing at present.
49	Additional Query	NA	Are you looking for 24*7 or 12*6 SOC monitoring, please clarify as this is required for adequate resource factoring.	10:00 am to 6:00 pm in all working days.
50	Additional Query	NA	Requesting tendering authority to clarify that TSDC will provison the complete compute infrastructure Server, VM, OS, DB, and Storage including Rack Space, Cooling, UPS, and Backup for hsoting all the required Security solution ?	Please refer corrigendum.
51	Additional Query	NA	Requesting tendering authority to clarify that... 1. TSDC will provision the complete compute infrastructure Server, VM, OS, DB, and Storage including Rack Space, Cooling, UPS, and Backup for hosting all the required Security solutions. 2. What is the minimum Logs and Events Stogare retention expected by TSDC for each solution, specifically for SIEM	Please refer corrigendum.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Sl. No.	Reference	Existing Clause	Query/ Request by Bidder	DIT Response
52	Additional Query	NA	Requesting tendering to look into this Since all the MNC OEMs will be having their Year-end closures in December end, it will be very difficult to get the required documentation from them by the 28th of December. Request that the submission date can be extended by at least 10 days from the current bid submission date, it will help us in getting a cost-effective solution for the mentioned scope.	Please refer corrigendum dated 28.12.2022

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Clause	Request by Bidder	Justification by Bidder	DIT Response
SECTION – XI 11.3 Annexure - III D. 5 Page 50	The SIEM solution should give insight into which systems communicated with each other, which applications were involved and what information were exchanged in the packets. By correlating this information with other network, log and user activity, it should be able to uncover abnormal network activity that may be indicative of compromised hosts, compromised users or data exfiltration attempts.	In the SIEM SOW the Packet capture is not asked, We would like to request TSDC team to include below mentioned points to enhance the functionality of Forensics through Packet Capture that have capability to do Deep Packet Inspection upto layer-7 using NTA along with Layer-2 to Layer-7 flow inspection to gain complete visibility and detect Zero Day/Unknown Threats. 1. Solution should support logs and Packets collection, correlation and alerts, have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack (Layer 2-7) including application payload data using NTA along with Layer-2 to Layer-7 flow inspection to gain complete visibility and detect Zero Day/Unknown Threats 2. Solution should capture packet at 100 Mbps and store RAW packet DATA for 5 days and normalized packet data for 10 days for forensics. 3. The solution should support full session reconstruction,session replay and object extractions from sessions like files and pcaps. 4. The solution must have the ability to capture network traffic and import PCAP files for analysis using the same infrastructure. 5. Solution should have unified console for threat detection using Logs and Packet Capture for compete correlation on all aspects. Solution should have the ability to convert traffic from raw packets to meaningful artifacts like email, FTP data files, VoIP conversations including PHP, JavaScript and .Net files. 6. Solution should create indexes for payload objects and not just rely on header information to augument investigation capabilities		No Change
SECTION – XI 11.3 Annexure - III D.6 Page 50	The SIEM Solution should support minimum 2000 Sustained Event Per Second (EPS) and should be capable of handling any Burst upto 5000 EPS without queuing or any log drop.	The SIEM Solution should support minimum 2000 Sustained Event Per Second (EPS) or 70 GB/Day (consider one event to be of 450 bytes and The EPS has to be uniform across all layers of Collection, Correlation and Management) . and should be capable of handling any Burst upto 5000 EPS without queuing or any log drop	We request to kindly confirm the retention time period for online and offile Log data to be considered. Also, Most of the market leading OEMs are providing licenses on per day data ingestion (GB/day) model	Please refer Corrigendum
SECTION – XI	The SIEM Solution licensing	The SIEM Solution licensing should be	Most of the market leading OEMs are	Please refer

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Clause	Request by Bidder	Justification by Bidder	DIT Response
11.3 Annexure - III D.7 Page 50	should be by the number of events per second, the solution must allow incoming events from at least 150, VMs, 150 physical servers / network devices/ security devices etc.	by the number of events per second or equivalent GB/Day, the solution must allow incoming events from at least 150, VMs, 150 physical servers / network devices/ security devices etc however, There should be no limitation on the number of devices to be supported. Any addition in number of devices should have no cost impact	providing licenses on per day data ingestion (GB/day) model. We would like to request TSDC to modify the clause as mentioned below - Also the License should not be dependent on number of devise to be integrated.	Corrigendum
SECTION – XI 11.3 Annexure - III D.10 Page 50	The Proposed SIEM solution should support the replay of historical data against the correlation engine to determine if the newly discover threats based on a new correlation rule has happened in the past.	-	The replay of data is possible if we provision Packets collection in the SIEM solution, we request to add the points as suggested by us to enhance and enable this functionality in the SIEM solution.	No Change
SECTION – XI 11.3 Annexure - III D.14 Page 51	OEM should be present in Gartner's Magic Quadrant for Security Information Event Management (SIEM) for atleast once in 2021 or 2020.	Remove	Kindly Requesting to give Exemption or Waive Off for this Clause that will allow the Indian Start ups such as ours and others an opportunity to participate in this opportunity.	No Change
		Remove	As there are equally good and competent OEMs in India as well. Also, as per the guidelines issued by the Central Government, Make in India OEMs should be given a platform as well.	No Change

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Clause	Request by Bidder	Justification by Bidder	DIT Response
SECTION – XI 11.3 Annexure - III D Page 50	Additional Suggestions/ Requests/ Queries	We suggest below clause as SIEM solution unsupported parser's become very critical in undermining the security threats. "The solution must provide a field extraction wizard that is used to create parsers and allow testing and validation with existing live or historical data within the system from the web interface. Solution should not be dependent on parser to ingest data. It should be able to ingest structured or unstructured data without a parser. If parser for data ingestion for any new data source /new version of data source is not available with OEM OOTB then OEM has to build and share the parser to Bidder within 15 days for duration of the contract."		No Change
		The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel. Same query string should be used for SBDL & SIEM.		No Change
		The proposed solution must be able to build an unstructured index or store data in its original format without any rigid schema. Solution should be provide a single console view where we can see all data whether metric or log event data and have a capability to correlate between the data sets.		No Change
		We suggest below clause to bring comprehensive Machine Learning functionalities in Next Gen SIEM The proposed solution must possess built-in function for Predictive Analysis: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modelling algorithms required to use this functionality, and the ability to easily interpret and customize the results		No Change
		Please confirm that TSDC will provide the necessary compute infra for installation of SEIM, SOAR or any other software specific to this tender or please mention the same needs to be provided by the bidder. However, If you can give 12 Core, 32 GB RAM with 1TB Storage VM in your Existing SDC it is sufficient for both SIEM and SOAR to be run on a single device/Server		Please refer Corrigendum
		Kindly confirm whether hardware for Software based SIEM solution, like Servers, VMs, OS, storage etc. will be provided by TSDC or bidder has to factor the same.		Please refer Corrigendum

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Clause	Request by Bidder	Justification by Bidder	DIT Response
		Do you require a Dedicated Server hardware / Appliance for this to be provided by the Bidder with the OS?		

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Clause	Request by Bidder	Justification by Bidder	DIT Response
SECTION – XI 11.3 Annexure - III A. 5 Page 47	The solution must have atleast the following modules, but not limited to, Antimalware, Host Based Intrusion Prevention System (HIPS), Host Based Firewall, Log Inspection, Data Leak Protection, Integrity Monitoring etc.	The solution must have atleast the following modules, but not limited to, Antimalware, Host Based Intrusion Prevention System (HIPS), Host Based Firewall, Log Inspection, Data Leak Protection, Integrity Monitoring etc.	The clause asks for Data Leak Prevention as part of Server Security which ideally is data protection regulation requirement.	Refer corrigendum.
SECTION – XI 11.3 Annexure - III A. 9 Page 47	The solution should have the capability to Monitor VM traffic	Kindly provide the use case for the same.		Any VM of CitrixZen Server, Hyper V, VMWare, etc
SECTION – XI 11.3 Annexure - III A.14 Page 47	Log Inspection module should provide the ability to collect and analyse operating system, databases and applications logs for security events.	Solution should be able to provide relevant logs for security events and remove log inspection module name	Today Endpoint security is evolved and EDR keeps the track of changes that occur on the system and accordingly prioritize the incident. For any specific incident if customer needs to collect the log , EDR has the capability to capture the required logs.	No Change
SECTION – XI 11.3 Annexure - III A.15 Page 47	Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.	solution should segregate alerts to low, medium and High	For wider participation of Top Level Gartner OEMs	No Change
SECTION – XI 11.3 Annexure - III A.19 Page 47	The solution should support Fail open & Fail close feature in HIPS.	Solution should be able to protect against exploits	Exploits covers all kind the malcious activities	No Change
SECTION – XI 11.3	The solution must provide advanced threat hunting features.	The solution must provide advanced threat detection- prevention feature and should integrate with custom on-premise sandbox	The clause asks for threat hunting capability in Server Security Solution which ideally is a part of EDR Solution.	Removed through corrigendum

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Clause	Request by Bidder	Justification by Bidder	DIT Response
Annexure - III		solution for IOC creation.		
SECTION – XI 11.3 Annexure - III A. 21 Page 48	The solution must provide by default security levels i.e. High, Medium & Low so that it eases the operational effort and it must have an option of assessment mode only so that URLs are not blocked but logged.	Could you please provide the exact use case here		No Change
SECTION – XI 11.3 Annexure - III A Page 47	Additional Suggestions/ Requests/ Queries	The solution should detect and block all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability) and should provide vulnerability shielding until actual patch is applied on the server		No Change
		The solution should be atleast EAL4 certified at anypoint of time & should provide CVE cross-referencing for vulnerabilities.		No Change
		The solution should automatically share suspicious samples with on premise custom sandbox solution for mitigation of zero-day threats		No Change
		The solution should protect against cross-site scripting (XSS) attacks & SQL injection attacks, central management server must able to support windows and linux for installtion.		No Change
		The solution should inspect SSL-encrypted HTTP traffic streams before they reach the application and protect web applications. It should support a wide variety of reports should be able to generate report data into a variety of different file formats like PDF,HTML etc.		No Change
		The solution should be among top four in IDC report for Server Security in any of last two published reports & should support atleast Windows family , Linux Family, etc.		No Change
		Query: Do you require a dedicated Server hardware with Operating System for this to be provided by the Bidder?		Refer corrigendum.
		Query: Breakup of Windows, Linux and CentOS OS Quantities		50 % windows and remainign are linux.

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Specification	Received Request	Justification by Bidder	DIT Response
SECTION – XI 11.3 Annexure - III H.19 Page 54	Threat Intelligence feed has to be unique and adhere to the dual incident monitoring design principle. Threat Intelligence feed from OEM other than the SIEM / SOAR OEMs is preferable	Need to rephrase as "Threat Intelligence feed has to be collobrative from all commerical as well as open source TI and adhere to the dual incident monitoring design principle. Threat Intelligence feed from propsed SIEM / SOAR OEMs is preferable	Threat Intelligence feed not getting intelligence from single source rather it takes from multiple TI sources and ingest consolidated feed to SOC. Threat Intelligence provides layered inteligence as well easy to integrate when provided from SIEM/SOAR vendor.	No Change
SECTION – XI 11.3 Annexure - III H.22 Page 54	Intelligence feeds should also preferably include feeds from the OEM providing the security hardware in-order to provide an integrated cyber-defense and data exchange between devices	Need to rephrase as "Intelligence feeds should have option to include feeds from the all leading threat intelligence vendors to provide an integrated cyber-defense and data exchange between devices.	Intelligence feed are hardware vendor neutral and having no correlation in terms of preference or providing any additional security intelligence benefits.	No Change
SECTION – XI 11.3 Annexure - III H Page 53	Additional Suggestions/ Requests/ Queries	Request you to add: Threat Intelligence Service should be from the same OEM of Server Security and AntiAPT. It should be built in onto these two services. Or if built in intelligence is not there then it has to comply as per RFP Spec.		No Change
		It should be Completely SaaS based Cloud Solution.		No Change
		Solution must tracks more than just IOCs, it focuses on attributes that are relevant to business such as Annualized Loss Expectancy (ALE), industry, impact, activity, discoverability,and effectiveness.		No Change
		Solution must provide threat visualization tool consist of global threat map, trending threats by industry, threats by region, industry, impact, etc.		No Change
		Solution should consumes up-to-date Threat Intelligence from the server, to formulate- Suspicious Addresses List Suspicious Domain List Suspicious Email List Suspicious Hash List Suspicious URL List		No Change
		Solution should have flash bulletins and created when a new cyber threat is identified, and posted on TI portal. TI Portal should let view the full writeup for any individual Flash Bulletin.		No Change

Response to the Queries made by the prospective bidders in connection to the RFP vide F.No.19(26)/DIT/SDC/2022 dated 07.12.2022

Reference	Existing Specification	Received Request	Justification by Bidder	DIT Response
		Solution should have capability to take Threat Intel Feed from open source (i.e. CRICL MISP) and other TI via STIX/TAXII		No Change
		Solution should equipped with reports which provide a comprehensive view of how threats operate, IOCs, key takeaways for the board, CISO,SOC, IT Ops, and Internal Auditing team.		No Change
		Solution should consist of portal which publishes bulletins, written to give a quick and simple overview of what is currently known about the threat, and basic steps to mitigate damage to your organization.		No Change
		Solution must have coverage to provide dashboard to immediately distinguished threats of lower magnitude and greater magnitude.		No Change
		Solution must provide real-time most relevant and actionable threat intelligence feed integrated with SIEM and SOAR.		No Change
		Solution enabled with threat advisory not only helps you learn about the threat and how it operates, but it will provide an overview diagram of its methods, detailed action plans for defense, and important takeaways for key roles throughout the organization.		No Change