Corrigendum

RFP for Selection of System Integrator for provision of DNS-DHCP-IPAM Solutions for Govt. of Odisha

RFP Ref No- OCAC-SEGP-INFRA-0002-2019-ENQ-23013

SL#	Clause	Existing Clause	Revised Clause
1.	Page No-6,Fact Sheet Point e on EMD	Earnest Money Deposit:₹15,00,000/- in shape of DD/RTGS or BG	Earnest Money Deposit:₹20,00,000/- in shape of DD/RTGS or BG
2.	Page no. 16 6.6.7 Tender Validity	Proposals shall remain valid for a period of 120 Days …	Proposals shall remain valid for a period of 180 Days …
3.	Page No-20, 7.1 Pre-Qualification Criteria	Point no. 4 : OEM Experiences The bidder/OEM must have successfully undertaken at least 5 heterogeneous setup (means BFSI, Government/ PSU/ Autonomous body, Telecom companies) the following numbers of similar assignments of value specified herein: - Minimum one project of similar nature, not less than the amount of ₹8,00,00,000/- (Eight Crore Only) or - Minimum two projects of similar nature, not less than the amount of ₹6,00,00,000/-(Six Crore Only) or - Minimum three projects of similar nature, not less than the amount of ₹4,00,00,000/-(Four Crore Only)	Point no. 4 : OEM Experiences The bidder/OEM must have successfully undertaken at least 5 heterogeneous environment setup (means BFSI, Government/ PSU/ Autonomous body, Telecom companies) the following numbers of similar assignments of value specified herein: - - Minimum one project of similar nature, not less than the amount of ₹6,00,00,000/- (Six Crore Only) or - Minimum two projects of similar nature, not less than the amount of ₹4,00,00,000/-(Four Crore Only) or - Minimum three projects of similar nature, not less than the amount of ₹2,00,00,000/-(Three Crore Only)
4.	Pg no-20,7.1 Pre-Qualification Criteria	Point no . 6 Quality Certification The bidder must possess a valid ISO 9001, ISO20001 & ISO27001 Certification.	Point no . 6 Quality Certification The bidder must possess a valid ISO 9001 & ISO27001 Certification.

5.	Page no. 23, Clause no. 7.3 Point a, e	(a)Bidders will be selected through Least Cost Based Selection Process (L1). (e) The Bidder, who has submitted the lowest Commercial bid (i.e. lowest in grand total), shall be selected as the L1 and shall be called for further process leading to the award of the assignment.	(a)Bidders will be selected through QCBS - Quality & Cost Based Selection with Technical and Financial ratio of 70:30. (e) The Bidder who will secure highest Composite Score will be awarded the work. The calculation of Technical, Commercial and Composite score as follows **<u>The formula for calculation of the Technical Score</u>** a) The bidder must comply to the specification to the items. b) The bidder with highest technical bid (H1) will be awarded 100% score c) Technical scores of other than H1 bidders will be evaluated using the following formula d) Technical Score of a Bidder = {(Technical Bid Score of the Bidder / Technical Bid Score of H1) X 100} % (Adjusted up to two decimal places) e) The Commercial bids of only the technically qualified Bidders will be opened for further processing. **<u>The formula for the calculation of the Financial Score</u>** a) The Financial Bids of the technically qualified bidders (those have secured more than 70% of mark in technical evaluation) will be opened on the prescribed date in the presence of bidders' representatives. b) The bid with lowest Financial (L1) i.e. "lowest price quoted" will be awarded 100% Score. c) Financial Scores for other than L1 Bidders will be evaluated using the following formula

			Financial Score of a Bidder= {(Financial Bid of L1/ Financial Bid of the Bidder) X 100} % (Adjusted up to two decimal Places) **The formula for the calculation of the Composite score** The technical and financial scores secured by each bidder will be added using weightage of 70% (Technical) and 30% (Financial) respectively to compute a Composite Bid Score. Bn = 0.70 * Tn + 0.30* Fn Where Bn = overall score of bidder Tn = Technical score of the bidder (out of maximum of 100 marks) Fn = Normalized financial score of the bidder The Bidder securing Highest Composite Bid Score will be adjudicated with the Best Value Bidder for award of the project.
6.	Page no. 22, 7.2.9 Technical evaluation scoring matrix		Technical evaluation scoring matrix (revised) See Annexure-I
7.	Pg no.:33, Schedule Deliverables	Sl No.1:Supply / Delivery of Software of the solution:T+12 weeks after the issue of the PO Sl No.2:Installation and commissioning:T+16 weeks	Sl No.1:Supply / Delivery of Software of the solution:T+16 weeks after the issue of the PO Sl. No.2:Installation and commissioning:T+20 weeks
8.	Pg no-36,9.8 Project Planning & Management	… DNS solution must support detecting common webserver CVEs detect and block. …	… The solution(OEM appliances) should be self-protected from any web attacks to avoid Mean Time to Failure(MTTF).

		The threat intelligence feeds should be available in multiple formats …	… The threat intelligence feeds should support future integration with all leading OEM of SIEM solutions. … (Other points remain unchanged)
9.	Pg no-37,9.9.2.2 External DNS Server	Point no. 5 The Solution must support 90,000 DNS QPS acting as an internal DNS Server	Point no. 5 The Solution must support 200000 DNS QPS for DC and for DR independently acting as External DNS Server. The Solution must support 200000 DNS QPS for DC and for DR independently acting as External DNS Server. The QPS calculated is the legitimate DNS Queries as we are looking for the DNS solution with DNS DDoS security which drop the DNS DDoS attack at the network interface level and only legitimate queries will be sent to the DNS engine for processing.
10.	Pg no-37,9.9.2.3 Internal DNS Server	Point no. 1 The Solution must support 75,000 QPS internal DNS servers.	Point no. 1 The Solution must support 125,000 QPS internal DNS servers.
11.	Pg no-40, 9.9.2.4 DHCP	1. The solution must provide an easy-to-use "import wizard" to import DHCP records from the legacy DHCP Solution. 2. Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines.	1. The solution must provide an easy-to-use "GUI based" to import DHCP records from the legacy DHCP Solution. 2. GUI based solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines. (other points remain unchanged)
12.	Pg no-49, 9.12 Bill of Materials		Revised Bill of Material Please see the Annexure-II of this corrigendum.
13.	Pg no-49,9.12	Appliance (External DNS) with Security (along with 1st year warranty and subscription)	Appliance (External DNS) with Security (along with 1st year warranty and subscription)

			Bidder has to propose appliance-based External DNS with active-active High availability cluster at DC and single instance at DR/BCP. Single instance of Hidden master should be provided at DC and DR.
14.	Pg no-49,9.12	Appliance (Internal DNS) with Security (along with 1st year warranty and subscription)	Appliance (Internal DNS) with Security (along with 1st year warranty and subscription) Bidder has to propose appliance-based Internal DNS with active-active High availability cluster at DC and single instance at DR/BCP
15.	Pg no-49,9.12	DHCP and IPAM License (along with 1st year warranty and subscription)	DDI appliance is meant for On-premises single OEM Solutions only
16.	Page no. 52 10.1.1 FORM PQ-1: Cover Letter	… Our proposal will be valid for acceptance up to 120 Days and I confirm … …	… Our proposal will be valid for acceptance up to 180 Days and I confirm … …
17.	Pg no-65, 10.3.2 Commercial bid		Please see the Annexure-III of this corrigendum.
18.	New Clause as per ICT Policy 2022 Govt. of Odisha		Consortium is not allowed. However, as per ICT policy of state of Odisha, the bidder shall mandatorily collaborate with a local enterprise having knowhow and experience in implementing similar projects for implementation (minimum of 25% for deployment and maintenance components).

Annexure-I

Technical Evaluation Scoring Matrix

Sl#	Evaluation Criterion	Maximum Marks	Documents Required
1	Implementation of Security solutions in any enterprise with order value of at least value of ₹2 crores during last 5 years (Security solution means implementation of Identity & Access management / SEIM solution/ DDI/ Firewall/ HSM/ Data Vault/ Security Operation Centre/ Zero Trust Networking etc.) Each Assignment will be awarded with 10 marks	20	Work completion/Go-live certificate or work order with self certification
2	Bidder's Experience in implementing of DDI Solution in any enterprise	10	Work completion/Go-live certificate or work order with self certification
3	Security Certified professionals engaged by bidder on a fulltime basis in its payroll. Following certifications shall only be considered CISA/ CISM/ CISSP/ OSCP/ ISO 27001/ OEM Certification relating to DDI solution For each ach Professional 2 marks will be awarded. (Maximum 10 Marks)	10	CV of employee Certified by the HR head with copy of the certification
4	Certification of the bidder ISO 27001 - 3 Marks ISO 20001 - 3 Marks SEI CMMi 5 - 4 Marks SEI CMMI 3 - 2 Marks	10	Valid copy of certificate.

5	**Technical Documentation and Presentation** Technical evaluation will be evaluated on the following parameters (apart from compliance with of the product quoted) : a. Design Architecture of ProposedSolution b. Resilience of proposed architecture,approach and methodology c. Future scalability d. Security Aspects Presentation and product demonstration on in-depth understanding of the proposed project's technical and functional requirements. Major Criteria fordemonstration (but not limited to) are given as under: • Bidder's understanding on project scope. • Bidder's knowledge and experience to deliver vis-à-vis scope of the assignment. • Project timeline, implementationframework on the proposed solution Bidder's ability to provide crisp and clear answers with strong content	50	– Technical document – Presentation andDemonstration

Annexure-II

Bill of Materials

Sl. #	Description	bidder to propose the quantity as per their solution	Unit
1.	Appliance (External DNS) with Security (along with 1st year warranty and subscription)		Nos
2.	Appliance (Internal DNS) with Security (along with 1st year warranty and subscription)		Nos
3.	Appliance (Hidden Master) with Security (along with 1st year warranty and subscription)		Nos
4.	DHCP and IPAM License (along with 1st year support and subscription)		Nos
5.	Central Management (along with 1st year support and subscription)		Nos
6.	Reporting and Analytics (along with 1st year support and subscription)		Nos
7.	Warranty support along with subscription of required Licenses for External DNS with security for 2nd year to 5th year	4	Years
8.	Warranty support along with subscription of required Licenses for Internal DNS with security for 2nd year to 5th year	4	Years
9.	Warranty support along with subscription of required Licenses for Hidden Master for 2nd year to 5th year	4	Years
10.	Warranty support along with subscription of required Licenses for DHCP and IPAM service for 2nd year to 5th year	4	Years
11.	Warranty support along with subscription of required Licenses for Central Management for 2nd year to 5th year	4	Years
12.	Warranty support along with subscription of required Licenses for Reporting and Analytics for 2nd year to 5th year	4	Years

13.	Deployment of one OEM certified Support staff (Initially for 24 months which may be extended further depending upon requirement)	24	Months
14.	Installation and Commissioning	1	Lumpsum
15.	OEM training for selected professionals of OCAC	20	officials
16.	Hardware relocation, installation & configuration cost(price discovery item)	1	Lumpsum
Note:	OCAC shall to provide nothing except Rack space, Power, connectivity. Hence, the bidder has to carefully mention the bill of material and quote accordingly		

- **The bidders have to mention the quantities as per the solution proposed by them with High availability active-active cluster at DC and single instance at DR/BCP**
- **The detailed solution architecture with diagram should be provided in Technical bid**
- **The bidder shall provide unpriced BoQ in technical bid otherwise the bid shall summarily be rejected.**
- **Bidder should furnish the datasheet of the product quoted with highlighting the specification mentioned in RFP.**
- **Besides, the OEM should furnish the product specification in OEM letterhead.**

Commercial bid (Revised)

Annexure-III

Sl#	Category	Quantity (Indicative)	Unit	Unit Cost (excluding GST)	Total cost (excluding GST)
A	B	C	D	E	F (C * E)
1	Appliance (External DNS) with Security (along with 1st year warranty and subscription)		Nos		
2	Appliance (Internal DNS) with Security (along with 1st year warranty and subscription)		Nos		
3	Appliance (Hidden Master) with Security (along with 1st year warranty and subscription)		Nos		
4	DHCP and IPAM License (along with 1st year support and subscription)		Nos		
5	Central Management (along with 1st year support and subscription)		Nos		
6	Reporting and Analytics (along with 1st year support and subscription)		Nos		
7	Warranty support along with subscription of required Licenses for External DNS with security for 2nd year to 5th year	4	Years		
8	Warranty support along with subscription of required Licenses for Internal DNS with security for 2nd year to 5th year	4	Years		
9	Warranty support along with subscription of required Licenses for Hidden Master for 2nd year to 5th year	4	Years		

10	Warranty support along with subscription of required Licenses for DHCP and IPAM service for 2nd year to 5th year	4	Years		
11	Warranty support along with subscription of required Licenses for Central Management for 2nd year to 5th year	4	Years		
12	Warranty support along with subscription of required Licenses for Reporting and Analytics for 2nd year to 5th year	4	Years		
13	Deployment of one OEM certified Support staff (Initially for 24 months which may be extended further depending upon requirement)	24	Months		
14	Installation and Commissioning	1	Lumpsum		
15	OEM training for selected professionals of OCAC	20	officials		
16	Hardware relocation, installation & configuration cost(price discovery item)	1	Lumpsum		
17.	Any other cost, bidder may specify				
				Grand Total (Excluding GST)	
Grand Total in words:					

(GST shall be applicable as per actual at the time of billing)

- Selection Method is Quality cum Cost-Based Selection (QCBS) with technical and commercial ratio of **70:30**
- The bid price will be exclusive of all taxes and levies and shall be in Indian Rupees.
- Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shallbe corrected. If there is a discrepancy between words and figures, the amount in words will prevail”.

Revised RFP Schedule

- **Last date of submission of bid : 28.04.2023 by 12 Noon**
- **Opening of Pre-qualification and Technical bid : 28.04.2023 by 12:30 PM**
- **Technical Presentation (by the bidders who are successful in pre-qualification criteria and quoted products are complied to required specification) : 04.05.2023 11:30 AM onwards through VC mode.**
- **Opening of commercial bid : To be intimated later**

Pre-Bid Resolution Document

SL#	Document Reference(s) (Section & Page Number(s))	Content of RFP requiring Clarification(s)	Points of clarification	OCAC Clarification
1	pg no-35,9.8 Project Planning & Management	Performance measurement and reporting features for each of: DNS, DHCP, database, management interface	Need help to clarify on clause for "database" is it refered to IPAM?	The "database" referred here is related to IPAM which should have an integrated database of DNS, DHCP and does not require any administration.
2	pg no-35,9.8 Project Planning & Management	Capacity measurement and reporting features for each of DNS, DHCP, database, management interface	Need help to clarify on clause for "database" is it refered to IPAM?	The "database" referred here is related to IPAM which should have an integrated database of DNS, DHCP and does not require any administration.
3	pg no-36,9.8 Project Planning & Management	DNS solution must support detecting common webserver CVEs detect and block	As Solution requested is DNS , DHCP & IPAM. There is no web security part of RFP. Request to remove this clause as DNS Server are not suppose to prevent Webservers CVEs	The solution(OEM appliances) should be self-protected from any web attacks to avoid Mean Time to Failure(MTTF).
4	pg no-36,9.8 Project Planning & Management	The threat intelligence feeds should be available in multiple formats	As Feeds are licenced & cannot be customized in formats. So request to remove this clause.	The threat intelligence feeds should support future integration with all leading OEM SIEM solutions.
5	pg no-37,9.9.2.2 External DNS Server	The Solution must support 90,000 DNS QPS acting as an internal DNS Server	Need clarity on DNS expected is for External Authoritative DNS & not Internal. Looks like typo error, need clarity. Also as OCAC is looking for scalable solution for 5 years, As understood before while studying the OCAC environment while peak of examination the session on Load-balancer use to peak to 160,000 session. We recommend the Solution performance number to be increase to 2,50,000 to deliver required traffic needs & able to sustain higher performance under DNS attack.	See the revised clause at corrigendum

6	pg no-38,9.9.2.2 External DNS Server	Ensure DNS and application availability and protection during DNS DDoS attacks or volume spikes. Mitigate DNS threats by blocking access to malicious IP domains based on reputational feeds.	Request to remove part of this clause "Mitigate DNS threats by blocking access to malicious IP domains based on reputational feeds." as this clause is more applicable towards Internal DNS functionality & should not be considered for External Authoritative DNS server functionality.	There are multiple incidents where coordinated attacks are generated on DNS Servers. Those domains should be automatically blocked in the External DNS DDoS security.
7	pg no-38,9.9.2.2 External DNS Server	22. Solution shall use technology to automatically update protection against new and evolving threats as they emerge to protect DNS service	This clause is more relevant for Internal Cache DNS Service for Automatic update & not relevant for External Authoritative DNS server. Request to remove or modify this clause.	The External DNS Security and updated controls should not have any manual intervention provisions (manual or Custom). New and evolving threat mitigation and analysis should be automatically updated in External DNS Security
8	pg no-38,9.9.2.3 Internal DNS Server	1. The Solution must support 75,000 QPS internal DNS servers	OCAC is looking for scalable solution for 5 years, As internal Application accessed east to west within OCAC environment would increase over period of 5 years which would lead to increase in DNS queries. So recommendation for solution performance number is to be increase to 1,00,000.	See the revised clause at corrigendum
9	pg no-39,9.9.2.3 Internal DNS Server	10. The vendor must have his own Threat Intelligence unit.	Request to change the clause to "The vendor must have his own or 3rd Party Threat Intelligence unit feeds"	AS per RFP

10	pg no-39,9.9.2.3 Internal DNS Server	15. The vendor shall have an in-house threat research team to provide real-time intelligence and depend on third-party feeds to enrich the threat feeds.	Request to change the clause to "The vendor shall have an in-house threat research team to provide real-time intelligence or depend on third-party feeds to enrich the threat feeds."	The threat intelligence research should be with OEM as in case of any false positive and any addition require in the threat intelligence the OEM should be capable in providing analysis of domain and IP address belongs to malicious nature. As per RFP
11	pg no-41,9.9.2.4 DHCP	41. The solution must be able to handle 450 DHCP Lease/sec	As mentioned in RFP on adoption of Modern Infrastructure for which DHCP play critical role of assisting IP Address. For 300,000 IP address we recommend OCAC to consider higher DHCP performance for at least 3000 DHCP Lease/sec	The DHCP is limited to end users' machines and does not apply to all 300,000 IP addresses. We also have remote offices. It is not possible that all lease requests will land on DHCP at the same point in time due to various latency factors. IA should have 12 hour lease period. The solution must be able to handle 500 DHCP Lease/s
12	pg no-44,9.11	The solution must provide signature-based, reputational-based, and behavioural-based security measures	Request to remove this clause as this clause is more applicable towards Internal DNS functionality & should not be considered for External Authoritative DNS server functionality.	There are multiple incidents where coordinated attacks are generated on DNS Servers. Those domains should be automatically blocked in the External DNS DDoS security. Also in case of any unknown threats on External DNS, the solution must be capable of using behaviour to block those attacks.
13	pg no-44,9.11	Ensure DNS and application availability and protection during DNS DDoS attacks or volume spikes. Mitigate DNS threats by blocking access to malicious IP domains based on reputational feeds.	Request to remove this clause as this clause is more applicable towards Internal DNS functionality & should not be considered for External Authoritative DNS server functionality.	There are multiple incidents where coordinated attacks are generated on DNS Servers. Those domains should be automatically blocked in the External DNS DDoS security.

14	pg no-45,9.11	The vendor must have his own Threat Intelligence unit.	Request to change the clause to "The vendor must have his own or 3rd Party Threat Intelligence unit feeds" which is already covered above in the Specifications.	The DDI and DNS Security should be with the same OEM for a smooth transformation to new technology. A single point of contact in case of any troubleshooting and administration. The multi OEM solution has interdependency and might take a longer time for resolution in case of any critical outage.
15	pg no-45,9.11	The vendor shall have an in-house threat research team to provide real-time intelligence and depend on third-party feeds to enrich the threat feeds.	Duplicate : Already covered above and needs to be removed.	As per RFP
16	pg no-49,9.12	Appliance (External DNS) with Security (along with 1st year warranty and subscription)	As per technical specs in External DNS mentioned in Section 9.11 - "The system proposed should be deployed 2 Qty at DC & 2 Qty at DR as a dedicated External Authoritative name server & 2 Qty of Hidden Master Server with 1 Qty at DC & 1 Qty at DR". We request for clarity on Qty proposed to be 2 Qty or 6 Qty?	See the revised clause at corrigendum
17	pg no-49,9.12	Appliance (Internal DNS) with Security (along with 1st year warranty and subscription) of 2 Qty	As per technical specs in External DNS mentioned in Section 9.11 - "The system proposed should be deployed 2 Qty at DC & 2 Qty at DR". We request for clarity on Qty proposed to be considered as 2 Qty or 4 Qty?	See the revised clause at corrigendum

18	pg no-49,9.12	DHCP and IPAM License (along with 1st year warranty and subscription)	As per technical Specs IPAM & DHCP server are mentioned of 2 Qty each. As best practice it is recommend to have DHCP & IPAM as separate instance. As DHCP is the production service which customer do not like to touch in production hours & IPAM is an operation & Management tool accessed multiple time for IP address management. IPAM should be separated from DHCP Server as requested in Technical specs.	See the revised clause at corrigendum
19	pg no-49,9.12	Central Management (along with 1st year warranty and subscription)	Central Management & Reporting function for some vendors are split on different instance & for some vendors Central Management & reporting runs together on IPAM. We would request to consider IPAM & Central Management & Reporting together.	DDI appliance is meant for On-prem single OEM Solutions only with Central Management
20	pg no-49,9.12	Reporting and Analytics (along with 1st year warranty and subscription)	Central Management & Reporting function for some vendors are split on different instance & for some vendors Central Management & reporting runs together on IPAM. We would request to consider IPAM, Central Management and Reporting together.	DDI appliance is meant for On-prem single OEM Solutions only including Reporting and Analytics.
21	Page No.6,Fact Sheet e) EMD	Earnest Money Deposit:₹15,00,000/- in shape of DD/RTGS or BG	Need Clarification as EMD amount of ₹20,00,000/- is also mention Page no:11 Pre Qualification section;Kindly clarify which EMD amount to be considered.	See the revised clause at corrigendum
22	7.2 Technical Evaluation Page No.88	Sl# Evaluation Criterion Max Score Documents Required i)	Need Clarification as Technical Scoring of Min 70 Marks is consider for evaluation process However Max 50 Marks Criteria has been published; Please Clarify	See the revised clause at corrigendum (Evaluation shall be made as per QCBS methodology)

23	7.1 Pre-Qualification Criteria Page No20	The bidder/OEM must have successfully undertaken at least 5 heterogeneous setup (means BFSI, Government/ PSU/ Autonomous body, Telecom companies) the following numbers of similar assignments of value specified herein: - Minimum one project of similar nature, not less than the amount of ₹8,00,00,000/- (Eight Crore Only) or - Minimum two projects of similar nature, not less than the amount of ₹6,00,00,000/-(Six Crore Only) or - Minimum three projects of similar nature, not less than the amount of ₹4,00,00,000/-(Four Crore Only)	Kindly Amend it to :The bidder/OEM must have successfully undertaken at least 5 (BFSI/Government/ PSU) IT Cybersecurity Projects with DNS/DDI as components herein: - Minimum one project of similar nature, not less than the amount of ₹8,00,00,000/- (Eight Crore Only) or - Minimum two projects of similar nature, not less than the amount of ₹6,00,00,000/-(Six Crore Only) or - Minimum three projects of similar nature, not less than the amount of ₹4,00,00,000/-(Four Crore Only)	See the revised clause at corrigendum
26	8.6 Performance Guarantee Page No:25	The bidder should furnish PBG amounting to 10% of work order value excluding tax in favour of OCAC valid for 68 months as per format attached at clause 10.3.4	Kindly Amend the PBG to 3% as it will help bidder to address the cost with reference to the scope of tender as Industry is yet to recover from Covid impact & Losses	As per RFP
27	Schedule Deliverables Page No:33	Sr No.1:Supply / Delivery of Software of the solution:T+12 weeks after the issue of the PO & Sr No.2:Installation and commissioning:T+16 weeks	Kindly Amend :Sr No.1:Supply / Delivery of Software of the solution:T+16 weeks after the issue of the PO & Sr No.2:Installation and commissioning:T+24 weeks	See the revised clause at corrigendum
28	9.14.1 Delivery, Installation and Commissioning Page No:50	Installation and commissioning: Within 4 weeks from the date of supply of materials	Kindly Amend :Installation and commissioning: Within 8 weeks from the date of supply of materials	See the revised clause at corrigendum
29	9.15 Payment term;Page No:51	9.15.1 Appliance Cost:a. 60% of the appliance cost on Delivery;20% of the appliance cost on Installation & Commissioning;Balance 20% of the appliance cost after 3 Month Successful run	Kindly Amend Payment it to atleast 80% Appliance cost in Delivery ;10% on Installation & 10% on Appliance cost after 3 Months successful runup	As per RFP

30	9.15 Payment term;Page No:51	9.15.2 License Cost 100% of the license cost shall be paid after Installation and commissioning.	Kindly Amend License cot to 80% on Delivery and rest 20% on Installation and Commissioning .As License are issue from Day 1.	As per RFP
31	9.15.3 Installation and Commissioning;Page No.:51	Payment of 70% successful running of the appliances and Balance 30% on after Successful running of the appliance and software for a period of three months	Kindly Amend payment it to 80% & 20% after Successful running of the appliance and software for a period of three months	As per RFP
32	7.1 Pre-Qualification Criteria;Page No:89	OEM should have implemented at least 5 heterogeneous setups (means BFSI, Government /PSU/Autonomous body, Telecom companies	Kindly Clarify if the Implementation of IT Cybersecurity Component can be considered apart from DHCP, DNS and IPAM (DDI) will be consider as pre qualification criteria	See the revised clause at corrigendum
33	9.15.5 Support Resource cost Page No.51	c. 100% of the payment towards cost of manpower resource shall be paid quarterly basis.	Kindly Confirm if the Payment is Quarterly Advance or Arrears ;If Arrear kindly make it Monthly Arrears	100% of the payment towards cost of manpower resource shall be paid quarterly basis after submitting all payment deliverables.
34	9 Terms of Reference (Scope of work);Page No.: 31	Effectively monitoring DNS traffic on your network for suspicious anomalies is critical to early detection of a security breach. By implementing State Level DNS, can keep an eye on all the important metrics. With intelligent **SIEM integration**	SIEM integration with proposed DDI are scope of Bidder ?	Yes, coordinating with SIEM team, SI needs to integrate DNS appliances
35	What is the retention period required for the Historical data. The reporting solution need to be sized accordingly.			As per the log retention policy, will keep the data.
36	Is the solution required to integrate with any other Security tool / Solution like NGFW, NAC, SIEM, SOAR ?			If required, respective team will facilitate the details and IA should integrate the same.
37	It is recommended that IPAM Solution integrate with Microsoft Active Directory for IP to user mapping. This will provide better visibility of end user in case of any compliance or security requirement.			As per RFP
38	RFP Page No. 6 / Point No. m RFP Page No. 16 / Point No. 6.6.7	Bid Validity Period - 180Days Tender Validity - 120 Days	We need to know what will be the actual Bid Validity?	See the revised clause at corrigendum

39	RFP Page No. 19 / Point No.2	The average annual turnover of the bidder during the last three financial year ending with 2021-22 should not be less than ₹ 40 Crore from IT/ITeS (as per the last published audited balance sheets / CA certified provisional balance sheet).	We are requested to modify through - The average annual turnover of the bidder during the last Four financial year ending with 2021-22 should not be less than ₹ 20 Crore from IT/ITeS (as per the last published audited balance sheets / CA certified provisional balance sheet).	As per RFP
40	pg no-49,9.12 Bill Of Materials	Warranty support along with subscription of required Licenses for additional 4 Years after 2nd Year onwards up to 5th Year against above appliances and licenses, Qty: 4 no.	As you asked for Additional warranty, support and subscription for 4 no. qty. only so above mentioned clarification required on actual no. of devices. Please clarify ?	See the revised clause at corrigendum Quantity should be proposed by the bidder as per their solution
41	9.9.2.1 General Requirement	8. DDI Solution proposed should be deployed on-prem & should have the ability to host cloud/SAAS-based solution.	8. DDI Solution proposed should provide on-prem services & should have the ability to provide services in the public-cloud	As per RFP
42	9.9.2.2 External DNS Server	9. The solution must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6).	How will the external DNS server use Forward and Stub zones?	The DNS Should support all the functionality of DNS protocols
43	9.9.2.2 External DNS Server	14. The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.	14. The Solution must support managed propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.	The Solution must support Instant and Custom propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.
44	9.9.2.2 External DNS Server	18. The system must be able to display all hosted DNS Resource Records in one GUI pane.	How and when will this feature be used? Is this for manually viewing and searching data, or for data export to another system?	The system must be able to display all hosted DNS Resource Records in one GUI pane as and when required. This is required for compliance and analysis perspective as well as it will help in ease of administration and operations
45	9.9.2.2 External DNS Server	19.The solution must support the standard DNSSEC specifications for serving of	Please explain "pass-through of client resolution". What are the queries that are being passed	The pass through means it should support DNSSEC validation

		DNSSEC-signed zones and the pass-through of client resolution of external zones.	through? Where will DNSSEC validation be performed?	
46	9.9.2.2 External DNS Server	21. The proposed solution must provide updates to the security protection rules and 22.Solution shall use technology to automatically update protection against new and evolving threats as they emerge to protect DNS service	Is it acceptable to have a SaaS component to the solution, so that security protection rules can be dynamically updated?	Yes, the threat intelligence and Threat update can be come from SaaS component using secure communication. But it is limited to update the on-premises. All the analysis and mitigation of security should be happen in On-premises DNS
47	9.9.2.2 External DNS Server	25. Ensure DNS and application availability and protection during DNS DDoS attacks or volume spikes. Mitigate DNS threats by blocking access to malicious IP domains based on reputational feeds.	Allowing DDoS attacks into your network can cause an outage in the network, even if your DNS server is unaffected, because your network is overloaded. Are you open to solutions that protect against DDoS outside of the DNS server itself?	The DNS should have ability to protect itself from any kind of DNS base DDoS attack and ensure continuous response during the attacks
48	9.9.2.3 Internal DNS	3. Solution should support standards-based DNS services on-prem & should not be a cloud-based Solution.	Is it acceptable to have a SaaS component to the solution?	Yes, the threat intelligence and Threat update can come from the SaaS component using secure communication. All the analysis and mitigation of security should happen in On-premises Only
49	9.9.2.3 Internal DNS	5. System should have a Cache DNS architecture to switch on demand from BIND to UNBOUND and vice versa.	Please explain the business requirements behind this technical requirement. Are you open to other solutions that meet the business requirements, other than the technical solution described in this requirement?	In case of any bind vulnerabilities, the IA should have the option to handle such issues without affecting the solution.
50	9.9.2.3 Internal DNS	11. The solutions must be able to deliver contextual awareness service and analysis to block threats from a dynamic set of high-risk IP addresses, to Detect malicious activities and sites and IP addresses	Please can you explain the background to this requirement?	The solution should have its own threat intelligence which consists of IP, Domain, etc and provide contextual information in case of any threat found.
51	9.9.2.3 Internal DNS	14.The behavior engine shall detect the DNS tunneling, anomaly and DNS	14.The behaviour engine shall detect the DNS tunnelling, anomaly and DNS	Behaviour analysis should help to protect from any unknown threats as

		exfiltration/infiltration automatically and once detected automatically apply policy using RPZ to block the communication	exfiltration/infiltration automatically and once detected, provide the ability to automatically block the communication	well as any data Exfiltration / infiltration which use DNS protocols like DNS tunnelling etc.
52	9.9.2.3 Internal DNS	16.The Proposed Recursive DNS should have the capability to secure from the below attacks.	16.The Proposed Recursive DNS should have the capability to secure against attack vectors that use DNS, such as: DNS Data Exfiltration, DNS cache poisoning attacks	As per RFP
53	9.9.2.3 Internal DNS	17. The Solution should be able to protect the Cache DNS Servers or freeze the DNS Cache content in the event of receiving a DDOS Attack even when the source of the attack cannot be identified.	17. The Solution should be able to respond from cache when external DNS resolution fails, when the required data is available, whether the failure is due to network problems caused by an attack, or any other outage of a required third-party external DNS service.	To ensure seamless DNS response even during attacks the solution should able to protect its cache
54	9.9.2.3 Internal DNS	26. System must support Anycast for DNS with BGP, IS-IS and OSPF.	26. System must support Anycast for DNS with BGP and OSPF.	As per RFP
55	9.9.2.4 DHCP	1. The solution must provide an easy-to-use "import wizard" to import DHCP records from the legacy DHCP Solution. 2. Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines.	I suggest the RFP should require the successful bidder to perform a successful migration from the legacy solution, (instead of requiring an "import wizard").	1. The solution must provide an easy-to-use "GUI based" to import DHCP records from the legacy DHCP Solution. 2. GUI based solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines.
56	9.9.2.4 DHCP	7. The solution must include an application programming interface (API) in order to interface with the network and/or asset management systems, a configuration management database (CMDB) solution or other applications.	Comment: This requirement could be strengthened, with specific requirements for the API.	The API is a very generic interface that helps the Client to integrate the solution with their existing tools. The requirement can be arrived in future so to ensure the solution should not have any show-stopper in the future with regards to API integration
57	9.9.2.4 DHCP	11.DDI IPAM user interface must be web-based without specific browser vendor requirements	11.DDI IPAM user interface must be web-based and support the current version of commonly used browsers	DDI IPAM user interface must be browser independent

58	pg no-20,7.1 Pre-Qualification Criteria	The bidder must possess a valid ISO 9001, ISO20001 & ISO27001 Certification.	Request you to please consider at least 2 of the last 3 Certification.	See the revised clause at corrigendum
59	pg no-25, 8.6 Performance Guarantee, Sl No-(b)	The bidder should furnish PBG amounting to 10% of work order value excluding tax in favour of OCAC valid for 68 months as per format attached at clause 10.3.4	We are request to reduce the PBG amount 10% to 3%. Suggestion: As per Government of India Ministry of Finance Department of Expenditure Procurement Policy Division OFFICE MEMORANDUM No. F.9/4/2020-PPD, it is decided to reduce Performance Security from existing 5-10% to 3% of the value of the contract for all existing contracts due to to the pandemic there is acute financial crunch among many commercial entities and contractors, which in turn is affecting timely execution of the contracts.	As per RFP
60	pg no-51, 9.15 Payment term	9.15.3 Installation and Commissioning Cost	a. 70% of the installation and commissioning cost shall be paid after Installation and commissioning. b. Balance 30% of the installation and commissioning shall be paid after successful running of the appliances and software for a period of three Months. Request: We are request to relax on this payment terms as Bidder is already submitted PBG on award of the contract for entire contract period & 20% Appliance Cost will be released after successful running for a period of three months We are request to change the clause as: 100% of the installation and commissioning cost shall be paid after Installation and commissioning.	As per RFP
61	pg no-36, 9.9 Functional requirements	Reporting Solution	Please clarify the retention period required for the Historical data. The reporting solution need to be sized accordingly	As per log retention policy, will keep the log.

62	pg no-43, 9.11 Specification and features	Reporting Solution	Please clarify the retention period required for the Historical data. The reporting solution need to be sized accordingly	As per log retention policy, will keep the log.
63	pg no-36, 9.8 Project Planning & Management	DNS solution must support to integration with ArcSight SIEM and SOAR from day one.	Is the solution required to integrate with any other Security tool / Solution like NGFW, NAC, SIEM, SOAR ? Request: We are request to add this in Clause 9.11 Specification and features of DDI Appliances with Licenses	As per RFP
64	pg no-37, 9.8 Project Planning & Management	DDI system must integrate with multiple pass-through authentication options including RADIUS, LDAP, Active Directory	OEMs are recommended, IPAM Solution should be integrate with Microsoft Active Directory for IP to user mapping. This will provide better visibility of end user in case of any compliance or security requirement. Request: We are request to add this in Clause 9.11 Specification and features of DDI Appliances with Licenses	As per RFP