

Corrigendum - Bid Reference No: DGR/WAF_SLB/2020/1				
SN	Tender/ATC Clause No.	Page No	Tender / ATC Clause detail	Revised Clause
1	5.2 Technical Specifications	19	10 vADC (Diff Conf,OS) from Day1 & Scalable to 20vADC ,L4 CPS- 2M ,L7RPS3.5M,SSL-30Gbps,L4-80Gbps,L760Gbps	10 vADC (Diff Conf,OS) from Day1 & Scalable to 15vADC ,L4 CPS- 1M ,L7RPS3.5M,SSL-30Gbps,L4-80Gbps,L760Gbps
2	4.12 Eligibility / pre-qualification criteria	13	Bidder should have minimum average annual turnover of Rs. 4 Crore from similar work only , in the last three financial years for which bidder's accounts have been audited.	Bidder should have minimum average annual turnover of Rs. 5 Crore in the last three financial years for which bidder's accounts have been audited.
3	5.3 Delivery, Installation & Commissioning	21	The delivery, installation & commissioning of the equipment should be completed within 45 days from the issue of Lol-cum-Work Order.	The delivery, installation & commissioning of the equipment should be completed within 60 days from the issue of Lol-cum-Work Order.
4	5.1.6	19	The equipment / solution would be tested for a minimum period of 15 days after installation & commissioning.	This clause stands deleted.
5	5.2 Technical Specifications	20	Web Application Security - 40K RSA-CPS or more 2k key or more & 25K ECC-CPS or more, Same OEM WAF that of LB , Standalone & virtualized mode, RAM-128GB or more	50K RSA-TPS or more 2k key or more & 30K ECC-TPS, or more, Same OEM WAF that of LB , Standalone & virtualized mode, RAM-128GB or more
6	5.2 Technical Specifications	20	Network Interface Ports - 6 *40G and 8*10G	Network Interface Ports - 4 *40G and 8*10G 40G SFPs- Optical 10G SFPs - 6 Optical, 2 Electrical
7	5.2 Technical Specifications	20	Attack Protection - OWASP TOP 10, AUTO POLICY, FINGERPRINTING / CAPTCHA, JavaScript challenge to client browser, HTML field Obfuscation, Protection from L7, BOT & automated attacks, Application Layer Encryption	Attack Protection - OWASP TOP 10, AUTO POLICY, FINGERPRINTING / CAPTCHA, JavaScript challenge to client browser, HTML field Obfuscation, Protection from L7, BOT & automated attacks
8	5.2 Technical Specifications	20	Power Consumption (Watt) - 400 Watt	This clause stands deleted.
9	5.2 Technical Specifications	20	Input-Output Port - Management Port; Console Port - RS232. Monitoring & policy through single GUI for WAF & ADC	Input-Output Port - Management Port; Console Port - RS232. Monitoring & policy through GUI for WAF & ADC
10	5.2 Technical Specifications	20	Compliance Certificates - ICSA LAB, NSS LAB, Forrester Leader/ Strong Performer For Indian OEM, EAL 2+ certification from STQC	Compliance Certificates - ICSA/NSS Lab

11	4.12.2 - 9.b	14	The solution being proposed must be current, based on latest technology and its end of sale date should not be within the next 2 years from the last date of submission of bids. Further, the OEM shall ensure the availability of spares for atleast 7 years.	The solution being proposed must be current, based on latest technology and its end of sale date, if announced, should not be within the next 1 year from the last date of submission of bids. Further, the OEM shall ensure the availability of spares for atleast 7 years.
12	5.2 Technical Specifications	20	Operating Humidity (%RH):95	This clause stands deleted.
13	8.7	33	In case of any one of equipment in HA mode is working and other is faulty due to any issue then Target / Service Level are "Within T0 + 36 hours of lodging of complaint".	In case of any one of equipment in HA mode is working and other is faulty due to any issue then Target / Service Level are "Within T0 + 72 hours of lodging of complaint".
14	Clause no. 4.12 Eligibility / pre-qualification criteria, Under 4.12.2, S N. 10	14	OEM should have successfully executed atleast three work orders of Web Application Firewall for government organizations during the last three years ending 31.01.2021.	OEM should have successfully executed three work orders of Web Application Firewall OR WAF + Server Load Balancer in Government / semi-Government / Private organizations during last three years ending 31.01.2021, each costing at least Rs. 1.5 crore. Supporting Documents – Copy of the related work orders confirming year, cost.

Response to Queries - Corrigendum - Bid Reference No: DGR/WAF_SLB/2020/1

SN	Firm's Name	ATC Clause No.	Page No	Tender / ATC Clause detail	Amendment Sought / Suggestion	Justification	PSeGS response
1	A10	5.2 Technical Specifications	19	10 vADC (Diff Conf,OS) from Day1 & Scalable to 20vADC,L4 CPS-2M,L7RPS3.5M,SSL-30Gbps,L4-80Gbps,L760Gbps	All the next generation platforms are approaching with container based Virtualization which creates isolated environments leveraging same OS to negate degradation in performance we request to remove Different OS mandate from compliance		Refer Corrigendum
2	Airtel	4.12 Eligibility / pre-qualification criteria	13	3. The bidder should have successfully completed "Similar Work" in government / large private organizations during the last three years ending 31.01.2021	Request Dept. to kindly revise the clause as below : " The bidder should have successfully completed "Similar Work" in government / large private organizations/PSU during the last three years ending 31.01.2021		Similar work in semi government organizations shall also be considered
3	Airtel	4.12 Eligibility / pre-qualification criteria	13	Bidder should have minimum average annual turnover of Rs. 4 Crore from similar work only, in the last three financial years for which bidder's accounts have been audited.	Request Dept. to kindly consider the minimum average annual turnover from IT/ITeS services since turnover specifically from the similar works is not mapped in the balance sheet of the bidder.		Refer Corrigendum
4	Airtel	4.12 Eligibility / pre-qualification criteria	13	4. Certificate from statutory auditors clearly certifying the turnover requirements	Request Dept. to kindly revise the clause as below : "Certificate from statutory auditors/practicing Chartered Accountant clearly certifying the turnover requirements"		As per Tender Document

5	Airtel	5.3 Delivery, Installation & Commissioning	21	The delivery, installation & commissioning of the equipment should be completed within 45 days from the issue of Lol-cum-Work Order.	Request Dept. to kindly revise the clause as below : "The delivery, installation & commissioning of the equipment should be completed within 90 days from the issue of Lol-cum-Work Order."		Refer Corrigendum
6	Airtel	5.1.2	19	The equipment / solution should be covered under 5 year onsite comprehensive OEM warranty. OEM must ensure 24 * 7 * 365 service support during warranty period through email, phone & web portal. Vendor is required to submit the details for the process of logging complaints	We assume bidder need to provide OEM Process details for logging complaints, kindly confirm		Complaint mechanism should fulfill the tender requirements.
7	Airtel	5.1.6	19	The equipment / solution would be tested for a minimum period of 15 days after installation & commissioning.	Bidder request DGRPG to amend this clause related to the solution timeline from 15 days to 7 days		Refer Corrigendum
8	Airtel	8	33	Submission of PBG & Signing of contract >>>15 days from the issue of Letter of Intent (Lol)-cum- Work orderRs. 2,000/- per day	request DGRPG to amend this clause as: Submission of PBG & Signing of contract >>>30 days from the issue of Letter of Intent (Lol)-cum- r"Submission of PBG & Signing of contract >>>Rs. 500/- per day"		As per Tender Document

9	Airtel	8	33	2. Delivery, Installation and Commissioning of WAF_SLB >>>2% of the total value of the contract per week for the delay.	Bidder request DGRPG to amend this clause as: "Delivery, Installation and Commissioning of WAF_SLB >>>0.5% of the total value of the contract per week for the delay with max capping to 5%."		As per Tender Document
10	Airtel	8	33	7. In case of any one of the equipment in HA mode is working and the other is faulty due to any issue >>> For a delay beyond 36 hours, a penalty @0.1% of the faulty equipment cost per day of delay (or part thereof) shall be applicable	Bidder request DGRPG to amend this clause as: "In case of any one of the equipment in HA mode is working and the other is faulty due to any issue >>> For a delay beyond 36 hours, a penalty @0.05% of the faulty equipment cost per day of delay (or part thereof) shall be applicable"		As per Tender Document
11	Airtel	8	33	8. In case both the equipment in HA mode are faulty due to any issue >>> For a delay beyond 24 hours, a penalty @0.2% of the contract value per day of delay (or part thereof) shall be applicable	Bidder request DGRPG to amend this clause as: "In case both the equipment in HA mode are faulty due to any issue >>> For a delay beyond 24 hours, a penalty @0.1% of the contract value per day of delay (or part thereof) shall be applicable"		As per Tender Document
12	Airtel	8	34	9. Preventive Maintenance of the equipment >>> <input type="checkbox"/> In case of non-compliance, a penalty @ Rs. 500 per day of delay shall be applicable.	Bidder request DGRPG to amend this clause as: "Preventive Maintenance of the equipment >>> <input type="checkbox"/> In case of non-compliance, a penalty @ Rs. 200 per day of delay shall be applicable."		As per Tender Document

13	Airtel	8	33	10. Repeated occurrence of the issues in equipment despite resolutions by the Service Provider >>> Rs. 5000 /- per day	Bidder request DGRPG to amend this clause as: "Repeated occurrence of the issues in equipment despite resolutions by the OEM >>> Rs. 1000 /- per day"		As per Tender Document
14	Airtel	6.11.1	25	The Client reserves the right to terminate, by prior written 2 months' notice, the whole or part of the contract, at any time for its convenience.	Request you to remove the clause of termination for convenience. Termination to happen only in case of default in the delivery of services / termination by paying the remaining payment in whole .		As per Tender Document
15	Airtel	8.7	33	In case of any one of equipment in HA mode is working and other is faulty due to any issue	Tat- T0+72 hours		Refer Corrigendum
16	Airtel	8.8	33	In case both the equipment in HA Mode are faulty due to any issue	Tat- T0+48 hours and Penalty @0.1%		As per Tender Document
17	Airtel	8.9	34	Preventive Maintenance of the equipment	It should be removed, Its is not required only.		As per Tender Document
18	Airtel	8.1	34	Repeated occurrence of the issues in equipment despite resolutions by Service provider	Within T0+45 days and Penalty at 1000 rs per day		As per Tender Document
19	Airtel	8.6	33	First response to the complaint	TAT T+2 Hrs and Penalty Rs 100 per Hour		As per Tender Document

20	Array	5.2 Technical Specifications	19	Deployment modes 10 vADC (Diff Conf,OS) from Day1 & Scalable to 20vADC,L4 CPS-2M,L7RPS-3.5M,SSL-30Gbps,L4-80Gbps,L7-60Gbps	Deployment modes 10 vADC (Diff Conf,OS, Dedicated CPU, memory, SSL core and HDD) from Day1 & Scalable to 20vADC,L4 CPS-2M,L7RPS- 3.5M,SSL-30Gbps,L4-80Gbps,L7-60Gbps, support third party network function on same appliance and standard VRRP for redundancy.	The specifications has been asked for vADC and WAF appliance with virtualization. The performance of each vADC is very critical and should provide guaranteed performance by having dedicated resources like CPU, SSL, Memory for each instance and as per open standard guidelines, it will be better if it can support third party and network function and standard VRRP as redundancy protocol.	Refer Corrigendum
21	Array	5.2 Technical Specifications	20	Web Application Security -40K RSA-CPS or more 2k key or more & 25K ECC-CPS or more, Same OEM WAF that of LB , Standalone & virtualized mode, RAM-128GB or more	Web Application Security - 100K RSA-CPS or more 2k key or more & 75K ECC-CPS or more, Same OEM WAF that of LB , Standalone / virtualized mode, RAM-128GB or more.	Considering the L7 through of 60 Gbps and HTTP Connections/Sec (Minimum) - 2M asked. As per today traffic trend and scenarios around 90-95% traffic is SSL. The SSL TPS is one of the most critical requirement so it should be inline with throughput and HTTP connection per sec.	Refer Corrigendum

22	Array	5.2 Technical Specifications	20	Network Interface Ports - 6*40G and 8*10G	Network Interface Ports -4*40G and 8*10G	As per current data center architecture and throughput asked , the required port of 40 G is very higher side and specific to an OEM. So it is suggested optimized number of ports required.	Refer Corrigendum
23	Array	5.2 Technical Specifications	20	Attack Protection - OWASP TOP 10, AUTO POLICY, FINGERPRINTING / CAPTCHA, JavaScript challenge to client browser, HTML field Obfuscation, Protection from L7, BOT & automated attacks, Application Layer Encryption	Attack Protection - OWASP TOP 10, AUTO POLICY, FINGERPRINTING / CAPTCHA, JavaScript challenge to client browser, HTML field Obfuscation, Protection from L7, BOT & automated attacks,	The application encryption feature is specific to one OEM and restricting other OEM to qualify. Each OEM has own way of securing the application from WAF prospective , application layer encryption is one way of protection but there are lot of other protection to protect the application. Application encryption is not feature of WAF but more of applications.	Refer Corrigendum
24	Array	5.2 Technical Specifications	20	Storage (GB) - 500 gigabytes	Storage (GB) - 4 TB	Considering the specifications of 20 vADC and WAF, the 500 GB HDD is not sufficient to keep the enhanced transactions log for 20 separate instances.	As per Tender Document

25	Array	5.2 Technical Specifications	20	Power Consumption (Watt) - 400 Watt	Power Consumption (Watt) - 400 Watt or more	Each OEM appliance power consumption depend on the architecture and performance of the device. It should be as industry standard not limited to 400 Watt, it depend on one 1U or 2 U device proposed.	Refer Corrigendum
26	Array	5.2 Technical Specifications	20	Input-Output Port - Management Port; Console Port – RS232. Monitoring & policy through single GUI for WAF & ADC	Input-Output Port - Management Port; Console Port – RS232. Monitoring & policy through GUI for WAF & ADC	Each OEM has own way for management for WAF and ADC whereas so it should be open and not specific clause,	Refer Corrigendum
27	Array	5.2 Technical Specifications	20	Compliance Certificates - ICSA LAB, NSS LAB, Forrester Leader/ Strong Performer For Indian OEM, EAL 2+ certification from STQC	Compliance Certificates - ICSA LAB, NSS LAB, Forrester Leader/ Strong Performer For Indian OEM, EAL 2+ certification from STQC/ make India Product	As per the guidelines from MoUD and MEITY, third party reports should not be used to restrict participation of vendors. We request you to refer DIPP and moD guide lines too for Make In India products .	Refer Corrigendum

28	CCS	4.5	29	EMD of amount of Rs. Eight Lakh only (Rs. 8,00,000/-) has been paid online	Being MSME/NSIC registered organization from Govt.of India, we request to competent authority to amend this clause to submit valid certificates of NSIC & MSME instead of deposit EMD and Tender fee and Ministry of Finance, Office memorandum number F.9/4/2020 PPD dated 12 November 2020 regarding Bid security/EMD stated that the Rule 171 of GFRs 2017 or any other Rule or any provision contained in the Procurement Manuals, no provisions regarding Bid Security should be kept in the Bid Documents in future and only provision for Bid Security Declaration should be kept in the Bid Documents.	Govt.of India promoting MSME organization's to participate in all types of e procurement/bidding for various sectors without submitting EMD and Tender cost while submitting valid NSIC & MSME valid certificates instead of submitting EMD and tender cost. Valid certicates with MSME letter is attached along with GOI office memorandum for your ready ref.	As per Tender Document
29	CCS	4.16	16	Performance security :The successful bidder shall furnish PBG to DGRPG valuing 10% of the contract value within 15 days of issue of Letter of Intent (LoI)-cum-Work Order.	Ministry of Finance, Office memorandum number F.9/4/2020 PPD dated 12 November 2020 regarding Performance security value reduced from 5% - 10% to 3% for all contracts.	We request to competent authority to reduce the Performance security value from 5-10 percentage to 3% for all contracts further against GOI circular issued. Govt. customer references with amendment of PBG value will be submitted if required from DGR.	As per Tender Document
30	CCS	5.1.4	19	Scope of Work: The proposed solution is required to be setup in High Availability (HA) mode	We requires information that whether it will be deployed in active/active or active passive mode.	Request for the Clarification against HA mode	Active-Active

31	CCS	New Addition Request	NA	Additional clause	Request to add clause for giving preference to ' Make In India Cyber Security Products /Solutions'and granting purchase preference to the Local manufacturer.	Request for the New addition in RFP clause for Make in India product Preference.	As per Tender Document
32	CCS	Eligibility / pre-qualification criteria - 3	13	The bidder should have successfully completed "Similar Work" in government / large private organizations during the last three years ending 31.01.2021 as per following details:- a One similar work costing not less than the amount equal to Rs. 3.5 Crore. OR b Two similar works each costing not less than the amount equal to Rs. 2.5 Crore each. OR c Three similar works costing not less than the amount equal to Rs. 1.5 crore each.	We understands that similar work includes all Data center equipments: Server, Storage, Firewall, NGFW , WAF and other cyber security products. Please clarify.	Request for the Clarification	Refer clause no.: 3.1.1.7
33	CCS	Eligibility / pre-qualification criteria - 4	13	Bidder should have minimum average annual turnover of Rs. 4 Crore from similar work only, in the last three financial years for which bidder's accounts have been audited.	We understands that similar work includes all Data center equipments: Server, Storage, Firewall, NGFW , WAF and other cyber security products. Please clarify.	Request for the Clarification	Refer clause no.: 3.1.1.7

34	CCS	Proof of Concept 4.14.3	16	The equipment for PoC has to be supplied by the bidder within 15 days of intimation failing which it would be deemed that the PoC has been unsuccessful and the bid would be rejected.	POC also need to be done in HA mode or will be acceptable in stand alone mode. Please clarify. POC has to be done on Premise or it will be acceptable in bidder/OEM premise.	Request for the Clarification	POC to be done in DGRPG premises and need not be in HA mode.
35	CCS	Technical Specifications 22	20	Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/ Strong Performer For Indian OEM, EAL 2+ certification from STQC	As per our understanding DGRP is not looking STQC certification for the equipment initially instead it is intended to be certified after deployment. Please clarify.	Request for the Clarification	Refer Corrigendum
36	CCS	Technical Specifications 22	20	Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/ Strong Performer For Indian OEM, EAL 2+ certification from STQC	STQC certification may take time as per the availability of auditors. We hope that delay due to STQC certification will not attract any penalty on bidder. Please clarify.	Request for the Clarification	Refer Corrigendum
37	CCS	5.2 Technical Specifications	20	Network Interface Ports - 6*40G and 8*10G	Please suggest No. of transceivers and type of transceivers of 40G and 10G required		Refer Corrigendum

38	CIPL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	19	1. Deployment modes: 10 vADC (Diff Conf,OS) from Day1 & Scalable to 20vADC, L4-80Gbps, L7-60Gbps	Deployment modes: 5 vADC (Diff Conf,OS) from Day1 & Scalable to 50vADC, L4-80Gbps/L7-60Gbps from day-1 and scalable upto L4-120Gbps/L7-100Gbps	Each application have different behaviour and shall be treated independently, virtualization feature will help here to create complete separate environment and isolation for different applications. The appliance should be scalable to meet all current and future requirements & simultaneously it should not be oversized as well.	Refer Corrigendum
39	CIPL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	20	2. Web Application Security: 40K RSA-CPS or more 2k key & 25K ECC-CPS or more, ,RAM-128GB or more	Web Application Security: 40K RSA-CPS 2k key & 25K ECC-CPS from day-1 and scalable upto 100K RSA-CPS 2k key & 45K ECC-CPS ,RAM-96GB and scalable upto 192GB	The appliance should be scalable to meet all current and future requirements & simultaneously it should not be oversized as well.	Refer Corrigendum

40	CIPL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	20	9. Attack Protection: Application Layer Encryption	Clause is deleted	Web Application Firewall should protect from known and unknown web application threats. It provides full security coverage out-of-the-box of OWASP Top-10 threats, including injections, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication, leakage of sensitive information and session management. Application Layer Encryption can't be part of WAF.	Refer Corrigendum
----	------	--	----	--	-------------------	--	-------------------

41	CIPL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	20	22. Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/Strong Performer For Indian OEM, EAL 2+ certification from STQC	Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/Strong Performer	<p>ICSA Lab is widely acceptable and provides third-party testing and certification of security and health IT products whereas EAL is common criteria certification, it does not measure the security of the system itself, it simply states at what level the system was tested. EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security. Such a situation may arise when securing legacy systems.</p> <p>Hence ICSA certification should be mandatory. Industry standard certification should also be considered to get healthy competition and right products.</p>	Refer Corrigendum
----	------	--	----	--	---	---	-------------------

42	CIPL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.3.1 Delivery, Installation & Commissioning	21	5.3.1 The delivery, installation & commissioning of the equipment should be completed within 45 days from the issue of Lol-cum-Work Order.	The delivery of the equipment should be completed within 60 days and installation & commissioning should be completed within 30 days from the issue of Lol-cum-Work Order.	Due to globally pandemic stitutaion mafucaturing, packing, transportation are impacted and expected delivery time from OEMs increased upto 8-10 Weeks	Refer Corrigendum
43	CIPL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 8 SLA and Penalties Sr. No. 2	33	Sr. No. 2 Delivery, Installation and Commissioning of WAF_SLB----- 45 days from the issue of Letter of Intent (Lol)-cum-Work order----- 2% of the total value of the contract per week for the delay.	Delivery, Installation and Commissioning of WAF_SLB----- 90 days from the issue of Letter of Intent (Lol)-cum-Work order----- 0.5% of the total value of the contract per week for the delay.	As per industrial practices this will be 0.5 % per week and maxiumum cap up to 10%	Refer Corrigendum

44	EDSPL	2.9	5	Earnest Money Deposit (EMD) through online mode - Rs. 8,00,000/-	Having pandemic situation and slow down in economy, would request you to please remove the EMD part and ask for declaration from bidders. Also, request you to please give relief to MSME partners.	Ministry of finance has issued notification in this regard to take bid security declaration in lieu of EMD. Notification has been attached along with the file. Notification No. No. F.9/4/2020-PPD Dated: - 12th Nov. 2020	As per Tender Document
45	EDSPL	4.16	16	The successful bidder shall furnish PBG to DGRPG valuing 10% of the contract value within 15 days of issue of Letter of Intent (LoI)-cum-Work Order.	Having pandemic situation and slow down in economy, would request you to please reduce the PBG from 10% to 3%.	Ministry of finance has issued notification in this regard to reduce PBG from 5-10% to 3%. Notification has been attached along with the file. No. F.9/4/2020-PPD Dated: - 12th Nov. 2020	As per Tender Document
46	EDSPL	5.3.1	21	The delivery, installation & commissioning of the equipment should be completed within 45 days from the issue of LoI-cum-Work Order.	Would request you to please change the no. of days from 45 days to 100 days.	These are high-end solutions and comes on back to back ordering basis. Lead time for the delivery of these devices are 60 days and installation would take 30-45 days.	Refer Corrigendum
47	EDSPL	6.4.2	22	97.5% payment will be made after delivery, installation, commissioning and training of the equipment & testing for minimum 15 days on production of following documents	Would request you to please keep 90% payment on delivery, 7.5% payment after installation, commissioning and training of equipment for 15 days.	Successful bidder will be submitting the PBG within 15 days from date of LOI as security. Therefore, request you to please accept our request.	As per Tender Document

48	F5	Deployment modes	19	10 vADC (Diff Conf,OS) from Day1 & Scalable to 20vADC,L4 CPS-2M,L7RPS-3.5M,SSL-30Gbps,L4-80Gbps,L7- 60Gbps	15 vADC(Diff Conf,OS) from Day1 & L4 CPS-1 M, L7RPS-3.5M, SSL-30Gbps, L4-80Gbps,L7-60Gbps	Considering the requirement of consolidating different departments' LB and WAF; the appliance must support minimum 15vADC from day1. Scaling up the vADC on the same platform based on license is proprietary and favourable to a single OEM. Considering other performance numbers, the L4 CPS is on a higher side and favoring single OEM so request you to reduce the CPS to 1 Million	Refer Corrigendum
49	F5	Web Application Security	19	40K RSA-CPS or more 2k key or more & 25K ECC-CPS or more, Same OEM WAF that of LB , Standalone & virtualized mode, RAM-128GB or more	75K RSA-TPS or more 2k key or more & 48K ECC-TPS, or more, Same OEM WAF that of LB , Standalone & virtualized mode, RAM-128GB or more		Refer Corrigendum
50	F5	HTTP Connections/Sec (Minimum) (Numbers)	20	HTTP Connections/Sec (Minimum) (Numbers): 2000000	HTTP Requests/Sec (Maximum) (Numbers)	Connections term are typically used as a reference point in Layer 4 of the OSI model. HTTP is factored on L7 requests per seconds or HTTP Requests per second	As per Tender Document
51	F5	Power Consumption (Watt)	20	Power Consumption (Watt): 400 Watt	Power Consumption (Watt): 500 Watt or less	Specific to single OEM.	Refer Corrigendum

52	F5	Operating Humidity (%RH)	20	Operating Humidity (%RH):95	Operating Humidity (%RH):95 or less	Specific to single OEM.	Refer Corrigendum
53	F5	4.12.2 - 10	14	OEM should have successfully executed atleast three work orders of Web Application Firewall for government organizations during the last three years ending 31.01.2021.- Work orders confirming year, cost and government organizations.	OEM should have successfully executed atleast three work orders of Web Application Firewall for government organizations during the last three years ending 31.01.2021.- Work orders confirming year and government organizations.	Typically PO is placed by customer to partner and partner places it on OEM ,thus the partner PO is to be considered and Work orders should be considered without cost as there is a NDA signed between OEM ,partner and customer for not disclosing the quoted amount	As per Tender Document
54	F5	4.12.2 - 9.b	14	The solution being proposed must be current, based on latest technology and its end of sale date should not be within the next 2 years from the last date of submission of bids. Further, the OEM shall ensure the availability of spares for atleast 7 years.	The solution being proposed must be current, based on latest technology. Further, the OEM shall ensure the availability of spares for atleast 7 years.	Hardware Support will be available for the duration of 7 years and since the procurement is going to happen in another 2-3 months then why EOS is relevant here as majority of the customer asks for the support availability for the term they want to buy and EOS is irrelevant. Request you to remove the EOS clause for 2 years from this clause as for few products EOS date is not yet declared.	Refer Corrigendum

55	Haldos, Ivanti	Clause no. 4.12 Eligibility / pre-qualification criteria, Under 4.12.2, S N. 10	14	OEM should have successfully executed atleast three work orders of Web Application Firewall for government organizations during the last three years ending 31.01.2021.	<p>Requesting to relax this clause as follows for an Indian OEMS :</p> <p>Should have successfully executed work orders of Web application Firewall or Similar work in India or globally with any Central Govt/Semi-Govt/ PSU/State Govt/ BFSI /Registered Companies/ Large private organisations during last three years ending 31.01.2021. We request you also to kindly consider following Govt. orders for allowing relaxation on Previous Experience criteria for Indian Cyber Security Companies :</p> <p>As per Govt. of India order- para no. 8 on page No. 4 of MEITY File No. 1(10)/2017-CLES dated 6th Dec 2019 (copy attached) says, "In any procurement process, the procuring entity shall not specify any mandatory qualification criteria, any eligibility specifications or certification(s) issued by any foreign testing/security lab(s)/analyst reviews which restricts eligibility of Indian cyber security products as defined in this order".</p> <p>Also, request you to refer to file No. P-45021/2/2017=PP (BE-II), Dept. of Promotion of Industry & Internal Trade, Ministry of Commerce and Industry, Government of India dated September 16th, 2020 Page Para no.10 (a & b) copy attached that says, Procuring entities shall endeavor to see that eligibility conditions in respect of previous experience, including on matters like turnover, production capability, and financial strength do not result in the unreasonable exclusion of local suppliers who would otherwise be eligible beyond what is essential for ensuring quality or creditworthiness of the supplier.</p>	Refer Corrigendum
----	----------------	---	----	---	--	-------------------

	56 Haltdos	Clause no. 5.2 Scope of Work/ Technical Specifications , Under Specifications , S N. 22, Compliance Certificates	20	ICSA LAB, NSS LAB, Forrester leader/ strong performer For Indian OEM, EAL 2+ Certification from STQC	<p>Requesting to relax this clause as follows for an Indian OEMS by allowing any one of following certifications : ICSA LAB/ NSS LAB/ Forrester leader strong performer/ For Indian OEM EAL 2+ Certification from STQC .</p> <p>We request you also to kindly consider following Govt. orders for allowing relaxation on Previous Experience criteria for Indian Cyber Security Companies :</p> <p>As per Govt. of India order- para no. 8 on page No. 4 of MEITY File No. 1(10)/2017-CLES dated 6th Dec 2019 (copy attached) says, "In any procurement process, the procuring entity shall not specify any mandatory qualification criteria, any eligibility specifications or certification(s) issued by any foreign testing/security lab(s)/analyst reviews which restricts eligibility of Indian cyber security products as defined in this order".</p> <p>Also, request you to refer to file No. P-45021/2/2017=PP (BE-II), Dept. of Promotion of Industry & Internal Trade, Ministry of Commerce and Industry, Government of India dated September 16th, 2020 Page Para no.10 (e) copy attached that says, "Specifying foreign certifications/ unreasonable technical specifications/ brands/models in the bid document is restrictive and discriminatory practice against local suppliers."</p>		Refer Corrigendum
--	------------	--	----	--	--	--	-------------------

57	Haltdos	Additional Clause	NA	Additional Clause	Request to add clause for giving preference to ' Make In India Cyber Security Products /Solutions'and granting purchase preference to Local manufacturer. Kindly refer to Ministry of Electronics and Information Technology order notification File No. 1(10)/2017-CLES dated 6th Dec, 2019 for Public Procurement (Preference to Make In India) order 2019 for Cyber Security Products and also refer to file No. P-45021/2/2017=PP (BE-II), Dept. of Promotion of Industry & Internal Trade, Ministry of Commerce and Industry, Government of India dated 16th September,2020 on the same.		As per Tender Document
58	Radware	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	19	1. Deployment modes: 10 vADC (Diff Conf,OS) from Day1 & Scalable to 20vADC	Deployment modes: 5 vADC (Diff Conf,OS) from Day1 & Scalable to 40vADC	Each application have different behaviour and shall be treated independently, virtualization feature will help here to create complete separate environment and isolation for different applications. The appliance should be scalable to meet all current and future requirements.	Refer Corrigendum

59	Radware	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	19	2. Web Application Security: RAM-128GB or more	Web Application Security: RAM-96GB from day-1 and scalable upto 192GB	Appliance should have capacity to meet current and future requirements, scalability should also be consider.	As per Tender Document
60	Radware	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	20	9. Attack Protection: Application Layer Encryption	Attack Protection: Application Layer Encryption/Sensitive Data Exposure Prevention	Web Application Firewall should protect from known and unknown web application threats. It provides full security coverage out-of-the-box of OWASP Top-10 threats, including injections, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication, leakage of sensitive information and session management. End to end sensitive data prevention functionality should be considered to secure the communications.	Refer Corrigendum

61	Radware	<p>Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications</p>	20	<p>22. Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/Strong Performer For Indian OEM, EAL 2+ certification from STQC</p>	<p>Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/Strong Performer</p>	<p>ICSA Lab is widely acceptable and provides third-party testing and certification of security and health IT products, as well as network-connected devices to measure product compliance, reliability and performance for most of the world's top technology vendors. EAL is common criteria certification, it does not measure the security of the system itself, it simply states at what level the system was tested. EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security. Such a situation may arise when securing legacy systems. There are Indian OEM who is ICSA Certified for other domain, hence ICSA certification should be mandatory. Industry standard certification should also be considered to get healthy competition and right products.</p>	Refer Corrigendum
----	---------	---	----	---	--	--	-------------------

62	SISL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	19	1. Deployment modes: 10 vADC (Diff Conf,OS) from Day1 & Scalable to 20vADC, L4-80Gbps, L7-60Gbps	Deployment modes: 5 vADC (Diff Conf,OS) from Day1 & Scalable to 30vADC, L4-80Gbps/L7-60Gbps from day-1 and scalable upto L4-120Gbps/L7-100Gbps	Each application have different behaviour and shall be treated independently, virtualization feature will help here to create complete separate environment and isolation for different applications. The appliance should be scalable to meet all current and future requirements & simultaneously it should not be oversized as well.	Refer Corrigendum
63	SISL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	20	2. Web Application Security: 40K RSA-CPS or more 2k key & 25K ECC-CPS or more, ,RAM-128GB or more	Web Application Security: 40K RSA-CPS 2k key & 25K ECC-CPS from day-1 and scalable upto 90K RSA-CPS 2k key & 40K ECC-CPS ,RAM-96GB and scalable upto 192GB	The appliance should be scalable to meet all current and future requirements & simultaneously it should not be oversized as well.	Refer Corrigendum

64	SISL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	20	9. Attack Protection: Application Layer Encryption	Clause is deleted	Web Application Firewall should protect from known and unknown web application threats. It provides full security coverage out-of-the-box of OWASP Top-10 threats, including injections, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication, leakage of sensitive information and session management. Application Layer Encryption can't be part of WAF.	Refer Corrigendum
----	------	--	----	---	-------------------	--	-------------------

65	SISL	Tender document for Supply, installation & Commissioning of WAF_SLB for PSDC Reference number: DGR/WAF_SLB/2020/1 5.2 Technical Specifications	20	22. Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/Strong Performer For Indian OEM, EAL 2+ certification from STQC	Compliance Certificates: ICSA LAB, NSS LAB, Forrester Leader/Strong Performer	ICSA Lab is widely acceptable and provides third-party testing and certification of security and health IT products whereas EAL is common criteria certification, it does not measure the security of the system itself, it simply states at what level the system was tested. EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security. Such a situation may arise when securing legacy systems. Hence ICSA certification should be mandatory. Industry standard certification should also be considered to get healthy competition and right products.	Refer Corrigendum
66	SISL	5.3.1 Delivery, Installation & Commissioning	21	5.3.1 The delivery, installation & commissioning of the equipment should be completed within 45 days from the issue of Lol-cum-Work Order.	The delivery, installation & commissioning of the equipment should be completed within 90 days from the issue of Lol-cum-Work Order.	OEM deliver will take around 75 days. Installation & commissioning to be consider for 15 days.	Refer Corrigendum

67	SISL	8. SLA and Penalties	33	7. In case of any one of the equipment in HA mode is working and the other is faulty due to any issue. Faulty equipment must be made functional in 36 hours.	Incase of any Hardware (RMA) issue. Replacement should be done in 72 hours.		Refer Corrigendum
68	SISL	8. SLA and Penalties	33	8. In case both the equipment in HA mode are faulty due to any issue. At least one equipment must be made functional in 24 hours.	Incase of any Hardware (RMA) issue. Replacement should be done in 72 hours.		As per Tender Document
69	SISL	EMD	5	EMD: Rs. 8,00,000 /- (Rs. Eight Lakh Only) through online mode	we request you to please refer memo number File no- No. F.9/4/2020-PPD issued by Ministry of Finance and accept bid securing declaration against EMD		As per Tender Document
70	SISL	PBG	16	The successful bidder shall furnish PBG to DGRPG valuing 10% of the contract value within 15 days of issue of Letter of Intent (Lol)-cum-Work Order.	We request you to please refer Memo No. F.9/4/2020-PPD issued by Ministry of finance against reduction of Performance security from 10% to 3% for all the contracts. Therefore, request you to please amend the clause accordingly.		As per Tender Document