Replies for Pre-bid queries: REQUEST FOR PROPOSAL (RFP) for Supply, Installation and Maintenance of IT Infrastructure for hosting PMMVY–CAS						
S. No.	**RFP Document Reference(s) [Section & Page Number(s)]**	**Content of RFP requiring Clarification(s)**	**Points of Clarification(s)**	**Change Requested**	**Bidder Name**	**MWCD's Response**
1	Page No-19, Clause No. 7. 1.4 (d)	Warranty should not become void, if MoWCD buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the Bidder. However, the warranty will not apply to such supplemental hardware items installed.	As per OEM standard if any third party component which is not certified by running Hardware OEM, will install in the device then warranty of the entire system may effects.		Bidder 1	As per RFP
2	Page No-95 & 96, Clause No .75 & 76	Minimum of 2x8 Core CPU, clock speed > 2.5GHz, latest generation intel processor , 2x600GB 15k RPM HDD , 4x 10Gb BaseT, 1xDP 16Gb FC HBA, RHEL, Free PCIe Slots for expansion	As per technical specs, you have mentions RHEL as OS for both type of Server , however in the Bill of Material mentioned on Page no.13, you are asking for Windows Server 2012 std. Please clarify the OS reuirement for each Server.		Bidder 1	Bidder will be supply,install and configure the OS. Please refer to bill of material for the licenses to be procured. Licenses will be open licenses. Bidder will also need to procure Redis licenses and install the same
3	Page No. 13, Clause No. 6. 1.1	Bill of Material : Server-2	Please clarify in which category this server will consider, Type-1 or Type 2 Server.		Bidder 1	Type 2
4	Page No. 95, Clause No. 75 & 76 (Network)	Should be configured with minimum 20 Gb connectivity per server with a minimum of 2 ports	As per Network clause you are asking for 20Gb connectivity using 2 Ports, however in the point no-1 of Server specs, you have menti		Bidder 1	Please refer to corrigendum point 6 & 7

			oned 4x 10G Base-T and 1x Dual port 16G FC. Please clarify which configuration you required.			
5	Page No. 97, Clause No. 77 SAN Storage	DISKS : Minimum 15 TB of useable capacity expandable up to minimum 25 TB, All Flash Storage with necessary hotspare	Please confirm the RAID type in which you want the usable capacity configured.		Bidder 1	Raid 5 with sufficient hot spare drives
6		SUPPORTED DRIVES : 300GB to 1.2 TB size / SAS (mandatory) and FC drives (optional)	As per this clause you are asking for SAS drives, but in the point no. 2 you have mentioned " All Flash Storage with necessary hotspare ". Please remove "All Flash Storage" word from the specs.		Bidder 1	please refer to Corrigendum point 2
7	Page No. 98, Clause No. 78 SAN Switch	Ethernet, RS232 and IP over Fiber Channel/ RJ-45 in-band over Fiber-Channel	Since you have already mentioned for management port in point no. 7, So please remove this clause.		Bidder 1	As per RFP
8	NEW CLAUSE	NEW POINT SUGGESTION	SIEM solution must integarte with all key IT infrastructire of Smart city and must have integartion with applications to pull security logs like SQL injection, XSS through agents. Even if aplication does not natively generate logs it must have a provision to pull logs and must not depend only on WAF for those logs.		Bidder 1	As per RFP

9	NEW CLAUSE	NEW POINT SUGGESTION	Proposed SIEM tool must be in existence for past 7 years atelast and should have evolved . OEM must not have declared its SIEM solution as end of life at anytime in last 7 years		Bidder 1	As per RFP
10	Section 36- point-i,pg-46		What will happen if any one product is not complied and still achieve 70%		Bidder 1	Bids with non-compliant products will be considered non-responsive
11	General query	technical compliance	What will happen if any one product is partially complied.		Bidder 1	All item should be fully complied
12	Page No-19, Clause No. 7.1.4 (d)	Warranty should not become void, if MoWCD buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the Bidder. However, the warranty will not apply to such supplemental hardware items installed.	As per OEM standard if any third party component which is not certified by running Hardware OEM, will install in the device then warranty of the entire system may effects.		Bidder 1	As per RFP
13	Page No-95 & 96, Clause No .75 & 76	Minimum of 2x8 Core CPU, clock speed > 2.5GHz, latest generation intel processor , 2x600GB 15k RPM HDD , 4x 10Gb BaseT, 1xDP 16Gb FC HBA, RHEL, Free PCIe Slots for expansion	As per technical specs, you have mentions RHEL as OS for both type of Server , however in the Bill of Material mentioned on Page no.13, you are asking for Windows Server 2012 std. Please clarify the OS reuirement for each Server.		Bidder 1	Please refer to section 6.1.1 bill of material
14	Page No. 13, Clause No. 6.1.1	Bill of Material : Server-2	Please clarify the function of server and in which category this server will fall, Type-1 or Type 2 Server.		Bidder 1	type 2

15	Page No. 95, Clause No. 75 & 76 (Network)	Should be configured with minimum 20 Gb connectivity per server with a minimum of 2 ports	As per Network clause you are asking for 20Gb connectivity using 2 Ports, however in the point no-1 of Server specs, you have mentioned 4x 10G Base-T and 1x Dual port 16G FC. Please clarify which configuration you required.		Bidder 1	As per RFP
16	Page No. 97, Clause No. 77 SAN Storage	DISKS : Minimum 15 TB of useable capacity expandable up to minimum 25 TB, All Flash Storage with necessary hotspare	Please confirm the RAID type in which you want the usable capacity configured.		Bidder 1	Raid 5 with sufficient hot spare drives
17		SUPPORTED DRIVES : 300GB to 1.2 TB size / SAS (mandatory) and FC drives (optional)	As per this clause you are asking for SAS drives, but in the point no. 2 you have mentioned " All Flash Storage with necessary hotspare ". Please remove "All Flash Storage" word from the specs.		Bidder 1	please refer to Corrigendum point 2
18	Page No. 98, Clause No. 78 SAN Switch	Ethernet, RS232 and IP over Fiber Channel/ RJ-45 in-band over Fiber-Channel	Since you have already mentioned for management port in point no. 7, So please remove this clause.		Bidder 1	As per RFP
19	Page No. 13 Clause No. 6.1.1 Bill of Material	ITIL Based Ticketing Tool & File Integrity Monitoring Tool has been asked in BOM.	We could not find hardware (Server) sizing for the same. in BOM asked.Need clarification on the harware resource provisioning for these two tools.		Bidder 1	Bidder has to propose as their solution requirement
20	Page No. 13 Clause No. 6.1.1 Bill of Material	Redis UAT Server (Type 1 Server) - As per Solution	We understands that Type 1 -server to be provided againast thisas we could n		Bidder 1	It will be a type 1 server with Redis solution installed

			ot find any referen ces for Redis server in solution UAT Ser ver need			
21	Page No. 14 C lause No. 7	The Bidder shall provide a d etailed methodology for pro viding these service at each of the locations of Ministry (HO, DC and DR). Bidder representatives shall be available for any meeting required with designated Ministry person nel or its representative.	We understand tha t at DC and DR syst em support service s will be required. Please clarify what kind of service will be required at HO .		Bidder 1	There is no r equirment of explicit servic es at HO but the successfu l bidder may be requried t o provide inc ident reports ,etc in HO
22	Page No. 16 C lause No. 7.1. 2.(n)	Bidder shall take backup, re move, protect, restore progr ams, data and remove stora ge media in a machine prior to presenting the machine f or service.	As Backup is not as ked from bider so we assume that ba ckup solution will b e provided by Mo WCD with all requir ed hardware, softw are and licences. Pl ease Clarify.		Bidder 1	If required th e backup sol ution will be provided by ministry
23	Page No. 20 C lause No. 7.1. 5.(b)	For implementing different versions of Application Soft ware, if adjustments / chang e in the configuration are to be made in base memory th e same should be carried ou t by the Vendor as a part of warranty.	We could not unde rstand it. Please ele borate it.		Bidder 1	Only applicat ion procured and installed by the bidder will be under the scope of preventive m aintainance
24	Page No. 26 C lause No.11(e)	The Bidder shall provide app ropriate training to the Mini stry's personnel or its design ee(s) to enable them to mai ntain infrastructure provide d under this RFP and subseq uent contract.	Please Clarify the n o. of participent an d No. of days in trai ning.		Bidder 1	This will be a t the time of the end of co ntract period as part of Kn owledge tran sfer and can not be assess ed currently
25	General Quer y		Bidder will deploy t he systems as aske d in RFP but applic ation migration will be done by MoWC D. Bidder will exten d all possible help f		Bidder 1	The understa nding is corr ect

			or the same. Bidder will not responsible for any changes in application if required in any case. Please Clarify.			
26	General Query		Racks, Power, Network Switches etc.. as required will be provided by MoWCD to deploy the asked equipments.		Bidder 1	Rack,Power and Network switches will be provided by NIC
27	Section 85 - Load Balancer, Page 110, Clause 2.6	IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation	Along with IPv6 support for DNS 64/46, it is critical that the LLB supports advanced DNS functions to achieve critical Inbound Load Balancing features. We recommend to change the clause to "**IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation. It should also support advanced functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc..**"		Bidder 1	As per RFP

28	Section 85 - Load Balancer, Page 110, Clause 3.1	Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode.	Some vendors use proprietary protocols for achieving HA which makes it difficult to troubleshoot or seamlessly integrate with parrallel/inline devices. To maintain interoperability and integration, we request to change the clause to "**Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode. The HA/Cluster shall be achieved using Standard VRRP (RFC 2338) and no proprietary protocols shall be used for the same.** "		Bidder 1	please refer to Corrigendum point 1
29	Section 85 - Load Balancer, Page 110, Clause 2.7	Domain name support for outbound link selection for FQDN based load balancing.	Along with Link Load Balancing and selection of the outbound link based on FQDN, the LLB should also support forward proxy deployments to sanitize the outgoing requests. We request you to change the clause to "**Domain name support for outbound link selection for FQDN based load balancing. The Appliance should also support acting as a Webagent service**		Bidder 1	As per RFP

			to implement explicit Forward proxy mode and to perform DNS Caching "			
30	Scope of Work , Sec 5 Page 11	Certification at two locations Delhi and Pune.	what kind of certification required?		Bidder 1	Certification includes the hardware and software acceptance procured, installed and configured by the bidder
31	Sec 6(m) Page 12	The bidder is required to procure, supply and install the required OS licenses as mentioned in Bill of Material	Can we bid server with OEM OS License installed?		Bidder 1	Licenses will be open licenses.
32	Sec 6.1.1 Page 13	OS	OEM OS License		Bidder 1	Licenses will be open licenses.
33	Sec 6.1.1 Page 13	APT Solution	Kindly mention qty		Bidder 1	DR-1 DC-1
34	Sec 6.1.1 Page 14	File Integrity Monitoring Tool	Kindly mention qty		Bidder 1	DC-1
35	Sec 7.1.4 Page 19	(a) Warranty should not become void, if MoWCD buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the Bidder. However, the warranty will not apply to such supplemental hardware items installed.	Remove this clause as this is not the standard terms.		Bidder 1	As per RFP
36	Payment Schedule Sec 13 A. 1. page no. 26	60% of the cost would be payable on delivery of the hardware	70% of the cost would be payable on delivery of the hardware		Bidder 1	As per RFP

37	Payment Schedule Sec 13 A. 1. page no. 26	1.25% of payment would be payable at the end of each quarter for 8 quarters across a period of 24 months or remaining 10% to be released after submission of PBG of equivalent amount.	Remove this clouse as 10% PBG are alr eady mentioned on page no. 50. sec 44 .		Bidder 1	Please refer to corrigendum point no. 4
38	Payment Schedule Sec 13 B. 1. page no. 27	Quarterly payments shall commence on completion of the warranty period and would be payable at the end of each quarter	All products are coming with 3 years warranty / ATS. So remove this clause.		Bidder 1	As per RFP
39	Summary of Cost 64.1.2 page no. 80	ATS/AMC Cost	All Products are coming with 3 years warranty / ATS. So AMC/ATS cost is not applicable.		Bidder 1	As per RFP
40	ATS/AMC OPEX 64.1.4 page no. 80	ATS/AMC Cost	All Products are coming with 3 years warranty / ATS. So AMC/ATS cost is not applicable.		Bidder 1	As per RFP
1	SAN Switch, Page -99	SWITCH BANDWIDTH : Minimum 250Gbps (full duplex)	The asked Bandwidth is very less for 16Gbps 48-port switch. Request to change this to " he switch offers full non-blocking 16-Gbps Fibre Channel performance on 48 line-rate ports and an aggregate bandwidth of 768 Gbps in each direction"		Bidder 2	As per RFP
2	SAN Switch, Page -99	Ethernet, RS232 and IP over Fiber Channel/ RJ-45 in-band over Fiber-Channel	Request to remove this spec. Not required		Bidder 2	As per RFP
3	SAN Storage, Page-98	CACHE : 4GB Controller cache with 72 hours battery back up	Pl change the specs as " 4GB per Controller cache "		Bidder 2	Please refer to corrigendum Point 5
4	SAN Storage, Page-98	DRIVE INTERFACE : 4 drive ports—Fiber Channel (FC) Switched and FC Arbitrated Loop (FC-AL) standard, auto-sensing 1Gbps/2 Gbps/4 Gbps	Pl change the Specs as" The Storage should support 12Gbps SAS Drive Ports " as now the technology has moved to		Bidder 2	Please refer to corrigendum point 16

			SAS			
5	SAN Storage, Page-98	HOST PORT : 4 no Switched FC or FC-AL/4 Gb/sec, 2 Gb/sec, 4 Gb/sec	Pl change this to : 4 x 16G FC Ports scalable upto 8 across Dual controllers		Bidder 2	Please refer to corrigendum point 6
6	SAN Storage, Page-98	MANAGEABILITY: The Storage Management Software shall be GUI Based and shall be able to discover and monitor storage systems. The management software shall be able to move data seamlessly within the storage box to different RAID groups or to other storage arrays connected to the virtualized /connected storage arrays without stopping the host applications. The storage management software provided shall conform to SNIA standards to avoid interoperability issues.	The storage will be able to move the data for virtual environement to other servers but not to other storage. Hence request to change the spec as below: "MANAGEABILITY: The Storage Management Software shall be GUI Based and shall be able to discover and monitor storage systems. The storage management software provided shall conform to SNIA standards to avoid interoperability issues."		Bidder 2	As per RFP
7	SAN Storage, Page-98	Add the spec in SAN Storage	The RFP has asked for 150K IOPS. We request to add the Flash Cache support in the storage for giving such high IOPS. Pl add _ " Offered Storage shall also support for Flash cache using SSD / Flash drives. Offered storage shall support at-least 8TB Flash Cache. Vendor shall offer atleast 1.6 TB Flash cache.		Bidder 2	Please refer to corrigendum Point 5

8	SAN Storage, Page-98	Add the spec in SAN Storage	Pl add that storage should be supplied with all the required software licences for the complete Array like Snapshot, clones, Replication licence, Thin provisioning licences etc needed for the operations		Bidder 2	As per RFP
		Minimum of 2x8 Core CPU, clock speed > 2.5GHz, latest generation intel processor , 2x600GB 15k RPM HDD , 4x 10Gb BaseT, 2xDP 16Gb FC HBA, RHEL, RHEL, Dual Power Supply, Free PCIe Slots for expansion	Minimum of 2x8 Core CPU, clock speed > 2.5GHz, latest generation intel processor , 2x600GB 15k RPM HDD , 4x10Gb **/ 2 x 20Gb ports**, 2x 16Gb FC HBA ports, RHEL.		Bidder 2	Please refer to corrigendum point 7 & 8
		Minimum of 2x12 Core CPU, clock speed > 3GHz, latest generation intel processor 256GB Ram ,2x600GB 15k RPM HDD , 4x10Gb BaseT, 2xDP 16Gb FC HBA, RHEL, RHEL, Dual Power Supply, Free PCIe Slots for expansion	Minimum of 2x12 Core CPU, clock speed > 3GHz, latest generation intel processor 256GB Ram ,2x600GB 15k RPM HDD , 4x10Gb **/ 2 x 20Gb ports**, 2x 16Gb FC HBA ports , RHEL.		Bidder 2	Please refer to corrigendum Point 8
1	Section 85 - Load Balancer, Page 110, Clause 2.6	IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation	Along with IPv6 support for DNS 64/46, it is critical that the LLB supports advanced DNS functions to achieve critical Inbound Load Balancing features. We recommend to change the clause to "**IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation. It should also support advanced functions Authoritative name sev**		Bidder 3	As per RFP

			er, DNS proxy/DNS NAT, full DNS serv er with DNSEC, DN S DDOS, applicatio n load balancing fr om day one. It sho uld be capable of h andling complete F ull DNS bind recor ds including A,MX, AAAA, CNAME, PT R, SOA etc.."			
2	Section 85 - L oad Balancer, Page 110, Cla use 3.1	Should provide comprehens ive and reliable support for high availability and N+1 clu stering based on Per VIP bas ed Active-active & active sta ndby unit redundancy mode .	Some vendors use proprietary protoc ols for achieving H A which makes it di fficult to troublesh oot or seamlessly i ntegrate with parra llel/inline devices. To maintain intero perability and integ ration, we request to change the claus e to "**Should provi de comprehensive and reliable suppo rt for high availabil ity and N+1 cluster ing based on Per VI P based Active-acti ve & active standb y unit redundancy mode. The HA/Clu ster shall be achiev ed using Standard VRRP (RFC 2338) a nd no proprietary protocols shall be used for the same.** "		Bidder 3	Please refer t o corrigendu m Point 1

3	Section 85 - Load Balancer, Page 110, Clause 2.7	Domain name support for outbound link selection for FQDN based load balancing.	Along with Link Load Balancing and selection of the outbound link based on FQDN, the LLB should also support forward proxy deployments to sanitize the outgoing requests. We request you to change the clause to "**Domain name support for outbound link selection for FQDN based load balancing. The Appliance should also support acting as a Webagent service to implement explicit Forward proxy mode and to perform DNS Caching** "		Bidder 3	As per RFP
4	Section 83 - WAF, Page 104, Clause 3.1	Should support 4 no's of 10/100/1000 Interfaces with integrated / external hardware bypass & 4 x 10G SFP+ SR ports	In considering any solution, scalability is of utmost importance. Hence, we request you to change the clause to "**Should support 4 no's of 10/100/1000 Interfaces with integrated / external hardware bypass & 4 x 10G SFP+ SR ports along with 2x40G QSFP+ Interfaces for future scalability**"		Bidder 3	As per RFP

5	Section 83 - WAF, Page 104, Clause 3.2	Should support 2TB of Storage space	Since WAF will be frontending all the critical/protected applications, a lot of scanning and memory intensive functions shall be performed on the WAF. Hence, we request to add the minimum RAM/Memory criteria as well. Please change the clause to "**Should support 2 TB of Storage space along with 64 GB RAM from Day 1.**"		Bidder 3	As per RFP
6	Section 83 - WAF, Page 105, Clause 4.3	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.	Each vendor caters to the Web vulnerability scanner in a different manner. Some OEMs have inbuilt capability and some vendors use separate Web Vulnerabily Scanners. Hence, to ensure wide participation, we request to change the clause to "**Should support an inbuilt/integrated Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.**"		Bidder 3	As per RFP
7	Section 83 - WAF, Page 105, Clause 4.23	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	"Fake Search Engine Request" is not an industry standard term and can be a terminology used by some specific OEM restricting wide participation. Request you to change the clause to "**Devic**		Bidder 3	As per RFP

			e should able to co ntrol BOT traffic an d It should able to block known bad b ots and fake searc h engine requests/ equivalent"			
8	Section 83 - WAF, Page 10 5, Clause 4.24	It should support scanning f or malicious content in uplo ads along with File upload vi olations and support integra tion with APT solution to sca n for zero day malwares.	Such integration wi ll require the WAF and APT solution fr om the same OEM which restricts the leading WAF OEMs to participate in th e tender as there is only one OEM havi ng both WAF and A PT Solution. Since, this clause is specifi c to a single OEM, r equest to relax the clause to "**It should support protection against Illegal File Upload/Download Volations**"		Bidder 3	Please refer t o corrigendu m Point 9
9	Section 83 - WAF, Page 10 6, Clause 9.1	Appliance should be able to terminate SSL	Since appliance has been asked to term inate SSL, sizing par ameters are very i mportant to qualify the hardware for t he requirement. W e request to chang e the clause to "**Ap plicance should be able to terminate SSL. The Appliance should support a minimum of 50,00 0 SSL TPS (RSA 2K Key) and 35,000 EC C TPS (ECDSA P256) from Day 1.**"		Bidder 3	As per RFP

10	Section 83 - WAF, Page 106, Clause 9.2	Should Passively decrypt SSL	Passive SSL Decryption is an obsolete technology and the latest one is Active decryption. Hence, we request to change the clause to "**Should Actively/Passively decrypt SSL**"		Bidder 3	As per RFP
11	Section 83 - WAF, Page 106, Clause 11.1	The product must possess a Web Application Vulnerability Scanning capability built in.	As mentioned previously, some vendors have inbuilt Web Application Vulnerabilty scanner and some have their WAF and their Scanner integrate as and when needed. Hence, for wider participation, we request you to change the clause to "**The product must support Web Application Vulnerability Scanning capability built-in or via integration**"		Bidder 3	Please refer to corrigendum point 10
12	Section 83 - WAF, Page 107, Clause 12.8	Should support and two Factor Authentication	Along with two factor authentication, it is critical to authenticate and allow only legitimate machines/endpoints to access the department's critical applications. Hence, we request to change the clause to "**Should support and two Factor Authentication. The solution should have license upgrade feature on same appliance to support machine authenticatio**		Bidder 3	As per RFP

			n based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access/authentication to critical resources."			
13	Section 83 - WAF, Page 107, Clause 13.3	Should support multiple log formats such as CSV, Syslog, TXT, etc..	Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change the clause to "**Should support multiple log formats such as CSV/Syslog/TXT etc.**."		Bidder 3	Please refer to corrigendum Point 11
14	Section 83 - WAF, Page 107, Clause 13.5	Should support report formats in PDF, HTML, WORD, RTF, etc..	Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change the clause to "**Should support report formats in PDF/HTML/WORD/RTF etc.**"		Bidder 3	Please refer to corrigendum Point 12
15	Section 84 - DDoS, Page no. 107 - Clause no. 4	Solution must support at least 8 x 1G LAN & 8 x 1G WAN interfaces	According to the RFP, the throughput asked is 6 Gbps and correspondingly, this clause asks for much higher number of interfaces. Request to change the clause to "**Solution must support at least 2 X 1G LAN & 2 X 1G WAN Interfac**		Bidder 3	As per RFP

			es and 2 X 10 GBE SFP+ Ports for futu re scalability"			
16	Section 84 - D DoS, Page no. 107 - Clause no. 5	Solution must at least suppo rt 6Gbps of Enterprise Mix tr affic	Since most of the t raffic is SSL based a nd the Anti-DDoS D evice needs to be S SL aware and ready , it is imperative to size the device wit h SSL/ECC Paramet ers as well. Hence, we request to chan ge the clause to "**S olution must at lea st support 6 Gbps of Enterprise mix T raffic. The applianc e should support a minimum SSL TPS (RSA 2K) of 20,000 and ECC TPS (ECDS A P256) of 14,000 f rom Day 1**"		Bidder 3	As per RFP
17	Section 84 - D DoS, Page no. 107 - Clause no. 8	The device should support h igh availability	As mentioned earli er, to ensure intero perability and easy troubleshooting pr ocess, the device s hould use industry standard protocols for HA. Hence, we r equest to change t he clause to "**The D evice should suppo rt high availability. The HA/Clustering should be based o n Standard VRRP (RFC 2338) and no proprietary protoc ols shall be used**"		Bidder 3	As per RFP

18	Section 84 - DDoS, Page no. 108 - Clause no. 18	The system must have an updated threat feed that describes new malicious traffic (botnets, phishing, etc...).	Every OEM has a different way of dealing with new and updated threat vectors. Some do it via threat feed and some vendors use a complete behavorial approach when detecting and mitigating threats. Hence, we request to relax the clause to "**The system must have an updated threat feed/On device Behaviour detection engine that describes new malicious traffic (Botnets, phishing, etc...)**"		Bidder 3	As per RFP
19	Section 84 - DDoS, Page no. 109 - Clause no. 42	It should be possible to block Geographical Locations to prevent flooding attacks from a particular country	This fuctionality can be either achieved using geography database or by using identifying geographies in the form of IP Ranges. Hence, we request relaxing the clause to "**It should be possible to block Geographical locations/Source IP Address/Source IP Ranges to prevent flooding attacks from a particular country**"		Bidder 3	As per RFP

20	Section 84 - DDoS, Page no. 109 - Clause no. 43	DDoS Appliance should receive a continuous update fed of Malicious Sources categorize as phishing, botnet etc	Every OEM has a different way of dealing with new and updated threat vectors. Some do it via threat feed and some vendors use a complete behavorial approach when detecting and mitigating threats. Hence, we request to relax the clause to "**DDoS Appliance should receive a continous update feed or should have an on-device behaviour engine of Malicious sources which can be categorized as phishing, botnet etc ...**"		Bidder 3	As per RFP
21	Section 81- SIEM,point-1,pg-112	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.	SIEM AND PACKET SHOULD BE TREATED AS SEORATE SOLUTIONS AND MUST INTEGRATE WITH EACH OTHER. PACKET CAPTURE IS VERY SPECIFIC REQUIREMENT AND HAVE DIFFERENT USE CASES THAT OF SIEM. THIS POINT IS PROPERITORY TO AN OEM WHO DOES UNIFIED SIEM WITH PACKET BUT DOES NOT GOVE PROPER OR COMPLTETE SOLUTION	NEXT GENERATION PLATFORM MUST INTEGRATE WITH SPECILAISED PACKET CAPTURE SOLUTIONS LIKE NIKSUN, SOLERA, EXINDA. MUST BE THREE TIER PHYSICALLY SEGREGATED ARCHITEURE CONSISTING OF LOG COLLECTION, LOG MANAGEMENT AND LOG CORRELATION ON PURP	Bidder 3	As per RFP

				OSE BUILT APPLIANCE /HARDWAR E WITH AD VANCED CA PABILITIES LIKE THREA T INTELLIG ENCE, USER ANALYTICS, APPLICATI ON ANALYT ICS		
22	Section 81- SI EM,point-2,p g-112	SIEM for Logs and deep pac ket inspection should be fro m same OEM.	SIEM AND PACKET SHOULD BE TREAT ED AS SEORATE SO LUTIONS AND MUS T INTEGRATE WITH EACH OTHER. PACK ET CAPTURE IS VER Y SPECIFIC REQUIR EMENT AND HAVE DIFFERENT USE CA SES THAT OF SIEM. THIS POINT IS PRO PERITORY TO AN O EM WHO DOES UN IFIED SIEM WITH P ACKET BUT DOES N OT GOVE PROPER OR COMPLTETE SO LUTION	SIEM AND PACKET SO LUTION M UST COME FROM DIFF ERENT OE M , SPECIA LISING IN E ACH AND MUST INTE GRATE FOR USE CASES TO BE DRIV EN	Bidder 3	As per RFP

23	Section 81- SIEM,point-8,pg-112	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.	LOGS ARE HIGHLY SENSITIVE AND ARE IN NUMBERS, HENCE ITS IMPORTANT TO PROTECT THEM AS WELL AS AGGREGATE AND COMPRESS.	LOGS MUST BE COMPRESSED ATLEAST 90%, MUST BE AGGREGATED AND FILTERED AT COLLECTOR LEVEL AND INGPROTECTED BY de-identify logs right at source through format peserving Encryption which should e NIST certified . The Solution should proide Field level encryption and decryption and based on roles the fileds should be decrypted based on roles . The Encryption algorith should make sure the Logs size is not increased and provides protection of Critical logs in rest, move and in use	Bidder 3	As per RFP

24	Section 81- SIEM,point-9,pg-112	A single log appliance should support minimum 10,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.	LOGS ARE IN GB/DAY AND MUST NOT BE MIXED WITH PACKETS AS BOTH ARE DIFFERENT	LOG MANAGEMENT APPLIANCE MUST BE 250GB/DAY ON PURPOSE BUILT APPLIANCE HAVING AT LEAST 128 GB RAM AND 12 TB OF INBUILT STORAGE PACKET APPLIANCE MUST BE SEPRATE AS PER NETWORK REQUIREMENT	Bidder 3	As per RFP
25	Section 81- SIEM,point-10,pg-112	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 20,000 EPS.	COORELATION IS ALWAYS FOR SECURITY THREATS BASED ON USE CASES HENCE LESSER AS COMPARED TO LOG MANAGEMENT WHERE ALL LOGS ARE CONSOLIDATED	CORRELATION LAYER MUST BE 5000 SUSTAINED/20000 PEAK EPS ON APPLIANCE WITH MINIMUM 192 GB RAM FOR OPTIMAL PERFORMANCE AND 1 MONTH OF ONLINE CORRELATED LOG STORAGE	Bidder 3	As per RFP
26	Section 81- SIEM,point-14,pg-113	Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.	COVERED ABOVE	CAN BE REMOVED AS COVERED ABOVE	Bidder 3	As per RFP
27	Section 81- SIEM,point-18,pg-113	Should be able to filter the captured packets based on layer- 2 to layer-7 header info	PROPERITORY TO OEM	SHOULD BE ABLE TO FILTER AND C	Bidder 3	As per RFP

		rmation.		APTURE LOGS BASED ON LAYER - 2 TO 7 HEADER INFORMATION		
28	Section 81- SIEM,point-19, pg-113	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.	PROPERITORY TO OEM	REQUEST TO BE REMOVED	Bidder 3	As per RFP
29	Section 81- SIEM,point-20, pg-113	The proposed solution must be able to provide the complete platform to perform Network forensics solution	LOG FORECSICS, WE ARE TALKING OF SIEM AND NOT NBAD. THESE POINTS SHOULD BE SEPRATE IN NBAD	THE PROPOSED SOLUTION MUST BE ABLE TO PROVIDE COMPLETE PLATFORM TO PERFOM LOG FORENSICS AND ANLYTICS	Bidder 3	As per RFP
30	Section 81- SIEM,point-21, pg-113	The solution must be able to detect malicious payload in network traffic	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 3	As per RFP
31	Section 81- SIEM,point-22, pg-113	• Detect and reconstruct files back to its original type	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 3	As per RFP
32	Section 81- SIEM,point-23, pg-113	• Detect hidden or embedded files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 3	As per RFP
33	Section 81- SIEM,point-24, pg-113	• Detect and flag out renamed files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 3	As per RFP
34	Section 81- SIEM,point-25, pg-113	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure .	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 3	As per RFP
35	NEW CLAUSE	NEW POINT SUGGESTION	SIEM solution must integarte with all key IT infrastructire of Smart city and must have integartion with applications to pull security logs like SQL injection, XSS through agents.		Bidder 3	As per RFP

			Even if aplication does not natively generate logs it must have a provision to pull logs and must not depend only on WAF for those logs.			
36	NEW CLAUSE	NEW POINT SUGGESTION	Proposed SIEM tool must be in existence for past 7 years atelast and should have evolved . OEM must not have declared its SIEM solution as end of life at anytime in last 7 years		Bidder 3	As per RFP
	Clause 77.3 Page no. 97	CACHE : 4GB Controller cache with 72 hours battery back up	CACHE : 32 GB Controller cache with 72 hours battery backup or cache de stage to SSD or equivalent technology to protect cache data in event of power failure	Storage to deliver 150,000 IOPS, controller cache minimum should be 32GB	Bidder 4	Please refer to corrigendum point 5
	Clause 77.4 Page no. 97	DRIVE INTERFACE : 4 drive ports—Fiber Channel (FC) Switched and FC Arbitrated Loop (FC-AL) standard, auto-sensing 1Gbps/2 Gbps/4 Gbps	DRIVE INTERFACE : 4 drive ports—SAS/ Fiber Channel (FC) Switched/FC Arbitrated Loop (FC-AL) standard, auto-sensing 3Gbps/6 Gbps/12 Gbps	As per current technology all vendors have SAS 12/6Gbps as drive interface	Bidder 4	Please refer to corrigendum point 16
	Clause 77.5 Page no. 97	HOST PORT : 4 no Switched FC or FC-AL/4 Gb/sec, 2 Gb/sec, 4 Gb/sec	HOST PORT : 4 no Switched FC or FC-AL/4 Gb/sec, 2 Gb/sec, 4 Gb/sec or Higher	As per current technology all vendors have FC 16Gbps as front end interface	Bidder 4	Please refer to corrigendum point 6

	Clause 77.13 Page no. 98	WAN Replication capability		Need Clarity does replication ports and license are required now ? replication ports 10G BaseT or 10G SFP+ depends up on customer existing LAN Switch type/ ports.	Bidder 4	As per RFP
	Clause 78.10 Page no. 98	NETWORK SERVICE : Up to 16 Virtual SAN, Fiber Channel ping and port level statistics	NETWORK SERVICE : Should support Virtual SAN/Virtual Fabric, Fiber Channel ping and port level statistics	Please get this change as requested to make generic to all SAN switch vendors	Bidder 4	As per RFP
1	Section 81- SIEM,point-1,pg-112	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.	SIEM AND PACKET SHOULD BE TREATED AS SEORATE SOLUTIONS AND MUST INTEGRATE WITH EACH OTHER. PACKET CAPTURE IS VERY SPECIFIC REQUIREMENT AND HAVE DIFFERENT USE CASES THAT OF SIEM. THIS POINT IS PROPERITORY TO AN OEM WHO DOES UNIFIED SIEM WITH PACKET BUT DOES NOT GOVE PROPER OR COMPLTETE SOLUTION	NEXT GENERATION PLATFORM MUST INTEGRATE WITH SPECILAISED PACKET CAPTURE SOLUTIONS LIKE NIKSUN, SOLERA, EXINDA. MUST BE THREE TIER PHYSICALLY SEGREGATED ARCHITEURE CONSISTING OF LOG COLLECTION, LOG MANAGEMENT AND LOG CORRELATION ON PURP	Bidder 5	As per RFP

				OSE BUILT APPLIANCE /HARDWAR E WITH AD VANCED CA PABILITIES LIKE THREA T INTELLIG ENCE, USER ANALYTICS, APPLICATI ON ANALYT ICS		
2	Section 81- SI EM,point-2,p g-112	SIEM for Logs and deep pac ket inspection should be fro m same OEM.	SIEM AND PACKET SHOULD BE TREAT ED AS SEORATE SO LUTIONS AND MUS T INTEGRATE WITH EACH OTHER. PACK ET CAPTURE IS VER Y SPECIFIC REQUIR EMENT AND HAVE DIFFERENT USE CA SES THAT OF SIEM. THIS POINT IS PRO PERITORY TO AN O EM WHO DOES UN IFIED SIEM WITH P ACKET BUT DOES N OT GOVE PROPER OR COMPLTETE SO LUTION	SIEM AND PACKET SO LUTION M UST COME FROM DIFF ERENT OE M , SPECIA LISING IN E ACH AND MUST INTE GRATE FOR USE CASES TO BE DRIV EN	Bidder 5	As per RFP

3	Section 81- SIEM,point-8,pg-112	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.	LOGS ARE HIGHLY SENSITIVE AND ARE IN NUMBERS, HENCE ITS IMPORTANT TO PROTECT THEM AS WELL AS AGGREGATE AND COMPRESS.	LOGS MUST BE COMPRESSED ATLEAST 90%, MUST BE AGGREGATED AND FILTERED AT COLLECTOR LEVEL AND INGPROTECTED BY de-identify logs right at source through format peserving Encryption which should e NIST certified . The Solution should proide Field level encryption and decryption and based on roles the fileds should be decrypted based on roles . The Encryption algorith should make sure the Logs size is not increased and provides protection of Critical logs in rest, move and in use	Bidder 5	As per RFP

4	Section 81- SIEM,point-9,pg-112	A single log appliance should support minimum 10,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.	LOGS ARE IN GB/DAY AND MUST NOT BE MIXED WITH PACKETS AS BOTH ARE DIFFERENT	LOG MANAGEMENT APPLIANCE MUST BE 250GB/DAY ON PURPOSE BUILT APPLIANCE HAVING AT LEAST 128 GB RAM AND 12 TB OF INBUILT STORAGE PACKET APPLIANCE MUST BE SEPRATE AS PER NETWORK REQUIREMENT	Bidder 5	As per RFP
5	Section 81- SIEM,point-10,pg-112	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 20,000 EPS.	COORELATION IS ALWAYS FOR SECURITY THREATS BASED ON USE CASES HENCE LESSER AS COMPARED TO LOG MANAGEMENT WHERE ALL LOGS ARE CONSOLIDATED	CORRELATION LAYER MUST BE 5000 SUSTAINED/20000 PEAK EPS ON APPLIANCE WITH MINIMUM 192 GB RAM FOR OPTIMAL PERFORMANCE AND 1 MONTH OF ONLINE CORRELATED LOG STORAGE	Bidder 5	As per RFP
6	Section 81- SIEM,point-14,pg-113	Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.	COVERED ABOVE	CAN BE REMOVED AS COVERED ABOVE	Bidder 5	As per RFP
7	Section 81- SIEM,point-18,pg-113	Should be able to filter the captured packets based on layer- 2 to layer-7 header info	PROPERITORY TO OEM	SHOULD BE ABLE TO FILTER AND C	Bidder 5	As per RFP

		rmation.		APTURE LOGS BASED ON LAYER - 2 TO 7 HEADER INFORMATION		
8	Section 81- SIEM,point-19, pg-113	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.	PROPERITORY TO OEM	REQUEST TO BE REMOVED	Bidder 5	As per RFP
9	Section 81- SIEM,point-20, pg-113	The proposed solution must be able to provide the complete platform to perform Network forensics solution	LOG FORECSICS, WE ARE TALKING OF SIEM AND NOT NBAD. THESE POINTS SHOULD BE SEPRATE IN NBAD	THE PROPOSED SOLUTION MUST BE ABLE TO PROVIDE COMPLETE PLATFORM TO PERFOM LOG FORENSICS AND ANLYTICS	Bidder 5	As per RFP
10	Section 81- SIEM,point-21, pg-113	The solution must be able to detect malicious payload in network traffic	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 5	As per RFP
11	Section 81- SIEM,point-22, pg-113	• Detect and reconstruct files back to its original type	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 5	As per RFP
12	Section 81- SIEM,point-23, pg-113	• Detect hidden or embedded files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 5	As per RFP
13	Section 81- SIEM,point-24, pg-113	• Detect and flag out renamed files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 5	As per RFP
14	Section 81- SIEM,point-25, pg-113	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure .	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 5	As per RFP
15	NEW CLAUSE	NEW POINT SUGGESTION	SIEM solution must integarte with all key IT infrastructire of Smart city and must have integartion with applications to pull security logs like SQL injection, XSS through agents.		Bidder 5	As per RFP

			Even if aplication does not natively generate logs it must have a provision to pull logs and must not depend only on WAF for those logs.			
16	NEW CLAUSE	NEW POINT SUGGESTION	Proposed SIEM tool must be in existence for past 7 years atelast and should have evolved . OEM must not have declared its SIEM solution as end of life at anytime in last 7 years		Bidder 5	As per RFP
1	Page No. 6056 Form 2: Compliance Sheet for Pre-qualification Proposal Point No. 9	The bidder should be either Original Equipment Manufacturer (OEM) of all IT assets in proposed BOM or their authorized partner in India for the last 5 years.	Please change the clause to The bidder should be either Original Equipment Manufacturer (OEM) of all IT assets in proposed BOM or their authorized partner		Bidder 6	Please refer to corrigendum point 13
2	Page 73 62.1.3 Form 8C: Letter for Qualifying as OEM or Authorized Partner	Form 8C: Letter for Qualifying as OEM or authorized partner: We, the undersigned, confirm that <name of bidding entity> are <Original Equipment Manufacturer (OEM) of all IT assets/offered components in proposed BOM> or <authorized partner in India for at least last 5 years of all IT assets/offered components in proposed BOM. Authorization letters from the Original Equipment Manufacturers (OEMs) / software copy right holders to this effect are attached herewith.	Please change as "We, the undersigned, confirm that <name of bidding entity> are <Original Equipment Manufacturer (OEM) of all IT assets/offered components in proposed BOM> or <authorized partner in India of all IT assets/offered components in proposed BOM. Authorization letters from the Original Equipment Manufacturers (OEMs) / software copy right holders to this ef		Bidder 6	As per RFP

			fect are attached herewith.			
3	General	Additional Clause	Please add this clause in Prequalification criteria Bidder should be CMMI V3 SVC		Bidder 6	As per RFP
4	General	Operating System	Please clarify the total count of the Microsoft OS and RHEL OS in servers.		Bidder 6	As per servers in BOM
5	Page No. 59 56 Form 2: Compliance Sheet for Pre-qualification Proposal	The Bidder should be a profit making entity with respect to operations in India in at least two of the three years preceding the last financial year. (Audited Financial statements for the financial years (FY 2014-15, 2015-16, 2016-17)	Please change the clause to The Bidder should be a profit making entity with respect to operations in India in last three years . (Audited Financial statements for the financial years (FY 2015-16, 2016-17, 2017-18)		Bidder 6	Please refer to corrigendum point 14
6	Page No. 60 56 Form 2: Compliance Sheet for Pre-qualification Proposal	The Bidder/Group Company/Parental Company must have implemented hardware and provided support to atlast 2 Government/ PSU client in last 5 years	Please change the clause to The Bidder must have implemented hardware and provided support to atleast 2 Government/ PSU client in last 5 years		Bidder 6	As per RFP

7	Page No. 61 56 Form 2: Compliance Sheet for Pre-qualification Proposal	The Bidder/Group Company must provide support at all locations of MoWCD – HO, DC and DR	Please change the clause to The Bidder must provide support at all locations of MoWCD – HO, DC and DR		Bidder 6	As per RFP
8	Page No. 98 77 SAN Storage	DRIVE INTERFACE : 4 drive ports—Fiber Channel (FC) Switched and FC Arbitrated Loop (FC-AL) standard, auto- sensing 1Gbps/2 Gbps/4 Gbps	Please change the clause to: DRIVE INTERFACE : 2 drive ports 12 Gbps SAS interface		Bidder 6	Please refer to corrigendum point 16
9	Page No. 98 77 SAN Storage	OS SUPPORT : Windows 200x, HP-UX(Optional) , Linux, AIX(Optional), Solaris	Please change the clause to: OS SUPPORT : Windows 200x, HP-UX(Optional) , Linux, AIX(Optional)		Bidder 6	As per RFP
10	Page No. 98 77 SAN Storage	AVAILABILITY: Redundant Power Supply and FAN. The storage array shall be an all-fiber technology and shall have all active components redundant to provide a No Single Point of Failure array architecture at any level	Please change the clause to: AVAILABILITY: Redundant Power Supply and FAN. The storage array shall have all active components redundant to provide a No Single Point of Failure array architecture at any level		Bidder 6	As per RFP
11	Page No. 98 77 SAN Storage	The storage system must support dynamic reconfiguration of file-system, its growth, dynamic reconfiguration of the logical volume across different controllers, and spanning of logical volumes across different controllers.	Please change the clause to: The storage system must support,dynamic reconfiguration of the logical volume across different controllers, and spanning of logical volumes across different controllers.		Bidder 6	As per RFP

12	Page No. 104 82 NGFW	The Firewall should have minimum 2 x 10G supporting SFP+ interfaces & 10x1G Base T RJ45 ports to cater to connectivity from multiple service providers and load balance them, Throughput should be 15 Gbps on 64 byte UDP packet size , IPSec Throughput of 10 Gbps, 250000 new session per second, 5M concurrent session, 3Gbps of SSL VPN throughput.The firewall should have redundant power supply.	The Firewall should have minimum 2 x 10G supporting SFP+ interfaces & 10x1G BaseT RJ45 ports .Throughput should be 20 Gbps on real world traffic , IPSec Throughput of 10 Gbps, 150000 new session per second;10 M concurrent session, .The firewall should have redundant power supply.The appliance should have 500Gb of internal storage to cater to the raw logs required for Audit.		Bidder 6	As per RFP
13	Page No. 104 82 NGFW	Features: Should support NAT64, DNS64 & DHCPv6, Traffic Shaping, should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 5 Virtual Firewall license should be provided and upgradation option up to 10 virtual Firewall should be there for Furture expansion, IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.	Features: Should support NAT64, Traffic Shaping, should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 5 Virtual Firewall license should be provided and upgradation option up to 10 virtual Firewall should be there for Furture expansion, IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.		Bidder 6	As per RFP
14	Page No. 104 82 NGFW	The Firewall & IPSEC modules shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification.	The Firewall & IPSEC modules shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification or should		Bidder 6	As per RFP

			NSS Recommended under NGFW categ ory in last 3 years.			
15	Page No. 104 82 NGFW	Intrusion Prevention System : IPS capability shall minimal ly attain NSS Certification, IC SA labs certication. 4 Gbps f or Enterprise Mix / Real wor ld traffic Throughput. Shoul d able to inspect SSL based t raffic. Should have atleast 7, 000 Signature.	Intrusion Preventio n System : IPS capa bility shall minimall y attain NSS Certifi cation, ICSA labs ce rtication. 1.5 Gbps for Enterprise Mix / Real world traffic T hroughput. Should able to inspect SSL based traffic.		Bidder 6	As per RFP
16	Page No. 104 82 NGFW	Threat Prevention : The Fire wall should have at least 4 G bps of Threat prevention thr oughput on Mix / real world traffic	Threat Prevention : The Firewall should have at least 1 Gbp s of Threat prevent ion throughput on Mix / real world tra ffic		Bidder 6	As per RFP
17	Page No. 83 WAF	Should support 2TB of Stora ge space	Please change the clause as: Solution should su pport 2TB of Storag e space		Bidder 6	As per RFP
18	Page No. 113 86 APT Soluti on	The solution should provide detection, analysis and rem ediation capability against A PT & SSL based APT attacks.	The solution shoul d provide detectio n, Prevention ;anal ysis and remediatio n capability against APT & SSL based A PT attacks.Should b e able to block eve n first zero day infe cted file.		Bidder 6	As per RFP
19	Page No. 113 86 APT Soluti on	The solution must employ a n on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and m ust not be signature based.	The solution must employ an on prem ise (not on cloud) a nalysis engine usin g virtual execution to detect zero day and unknown thre ats and must not b e signature based.T		Bidder 6	As per RFP

			he solution should be able to deliver clean file by removing any zero day malware (if) attached with MS Document.			
20	Page No. 113 86 APT Solution	common multimedia contents such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zeroday attacks.	common multimedia contents such as JPEG/GIF/WMF and ZIP/RAR/7ZIP archives to prevent advanced Malware and Zeroday attacks.		Bidder 6	As per RFP
21	Page No. 113 86 APT Solution	The proposed solution should support SMB / CIFS / NFS protocol for sharing and transferring files	The proposed solution should support SMB / CIFS protocol for sharing and transferring files		Bidder 6	As per RFP
22	Page No. 113 86 APT Solution	Number of VM's should be atleast 56 from day 1	Number of VM's should be atleast 30 from day 1 with 3.5 Gbps capacity		Bidder 6	As per RFP
23	Page No. 113 86 APT Solution	The APT appliance should be able to process minimum of 1000 files/hour (either web or network or both) on the VM sandboxing	The APT appliance should be able to process minimum of 2000 files/hour (either web or network or both) on the VM sandboxing		Bidder 6	As per RFP
24	Page No. 114 87 File Integrity Monitoring Tool	The monitoring speed should be upto 500k files in 10 seconds at File level.	Please change the clause to : Solutions should provide file monitoring and tamper protection at a fast rate.		Bidder 6	As per RFP
25	Page No. 114 87 File Integrity Monitoring Tool	If tampered file is detected, it must be recovered automatically within 1 min	Please change the clause to : Solution should provides tamper protection and records the changes made to the file		Bidder 6	As per RFP
26	Page No. 114 87 File Integrity Monitoring	Data Recovery	Please Remove this spec it is OEM specific		Bidder 6	As per RFP

	Tool					
27	Page No. 114 87 File Integrity Monitoring Tool	Auto Recovery	Please Remove this spec it is OEM specific		Bidder 6	As per RFP
28	Page No. 114 87 File Integrity Monitoring Tool	KSI Block Chain	Please Remove this spec it is OEM specific		Bidder 6	As per RFP
29	Page No. 114 87 File Integrity Monitoring Tool	The technology should work on “keyless” signature to any type of data.	Please Remove this spec it is OEM specific		Bidder 6	As per RFP
1	Page No. 27 Payment Schedule	Supply of hardware/System Software at DC and DR and Signed Off BOM Verification report	60% of the cost would be payable on delivery of the hardware	We request you to kindly amend this clause as - 80% of the cost would be payable on delivery of the hardware.	Bidder 7	As per RFP As per RFP
		Commissioning of Hardware / System Software Installation	20% of the delivered hardware cost would be payable on successful installation of the hardware/ System Software	We request you to kindly amend this clause as - 10 % of cost would be payble on Installation commisioning and project-go live.	Bidder 7	As per RFP
		Verification and sign-off post commissioning	10% of the cost will be payable post-go-live after complete PMMVY-CAS setup is migrated to new infrastructure			As per RFP
		Quarterly payment	1.25% of payment would be payable at the end of each quarter for 8 quarters across a period of 24 months or remaining 10% to be released after submission of PBG of	1.25% of payment would be payable at the end of each quarter for 8 quarters across a period of 24 mo	Bidder 7	Please refer to corrigendum point 4

			equivalent amount	nths or remaining 10% to be released after submission of PBG of equivalent amount.These changes are request to participation of Multiple SI and to execute the project smoothly.		
2	**Clerification**	As per RFP understanding no Top Of rack switches asked in Solution. Kindly Clear the Blade Chassis swites will be directly connected to NIC DC Switch or SI has to consider Two Nos of TOR switches also. If SI has to consider please include the TOR switches specifications in RFP.			Bidder 7	As per RFP
3	Section 85 - Load Balancer, Page 110, Clause 2.6	IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation		Along with IPv6 support for DNS 64/46, it is critical that the LLB supports advanced DNS functions to achieve critical Inbound Load Balancing features. We recommend to change the clause to "**IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation. It should also support ad**	Bidder 7	As per RFP

			vanced fun ctions Auth oritative n ame sever, DNS proxy/ DNS NAT, f ull DNS ser ver with D NSEC, DNS DDOS, appl ication loa d balancing from day o ne. It shoul d be capabl e of handli ng complet e Full DNS bind record s including A,MX, AAA A, CNAME, PTR, SOA e tc.."		
4	Section 85 - L oad Balancer, Page 110, Cla use 3.1	Should provide comprehensive and reliable sup port for high availability and N+1 clustering base d on Per VIP based Active-active & active standb y unit redundancy mode.	Some vend ors use pro prietary pr otocols for achieving H A which ma kes it diffic ult to troub leshoot or s eamlessly i ntegrate wi th parrallel /inline devi ces. To mai ntain intero perability a nd integrati on, we req uest to cha nge the cla use to "**Sho uld provide comprehen**	Bidder 7	Please refer t o corrigendu m point 1

			sive and rel iable supp ort for high availability and N+1 cl ustering ba sed on Per VIP based Active-acti ve & active standby un it redunda ncy mode. The HA/Clu ster shall b e achieved using Stan dard VRRP (RFC 2338) and no pro prietary pr otocols sha ll be used f or the sam e."		
	Section 85 - L oad Balancer, Page 110, Cla use 2.7	Domain name support for outbound link selecti on for FQDN based load balancing.	Along with Link Load B alancing an d selection of the outb ound link b ased on FQ DN, the LLB should also support for ward proxy deploymen ts to sanitiz e the outgo ing request s. We requ est you to c hange the c lause to "**D omain nam e support f or outboun**	Bidder 7	As per RFP

			d link selection for FQDN based load balancing. The Appliance should also support acting as a Web agent service to implement explicit Forward proxy mode and to perform DNS Caching "		
	Section 83 - WAF, Page 104, Clause 3.1	Should support 4 no's of 10/100/1000 Interfaces with integrated / external hardware bypass & 4 x 10G SFP+ SR ports	In considering any solution, scalability is of utmost importance. Hence, we request you to change the clause to "**Should support 4 no's of 10/100/1000 Interfaces with integrated / external hardware bypass & 4 x 10G SFP+ SR ports along with 2x40G QSFP+ Interfaces for future scalability**"	Bidder 7	As per RFP

	Section 83 - WAF, Page 104, Clause 3.2	Should support 2TB of Storage space	Since WAF will be fronting all the critical/ protected applications, a lot of scanning and memory intensive functions shall be performed on the WAF. Hence, we request to add the minimum RAM/Memory criteria as well. Please change the clause to "**Should support 2TB of Storage space along with 64 GB RAM from Day 1.**"	Bidder 7	As per RFP
	Section 83 - WAF, Page 105, Clause 4.3	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.	Each vendor cater to the Web vulnerability scanner in a different manner. Some OEMs have inbuilt capability and some vendors use separate Web Vulnerabily Scanners. Hence, to ensure wid	Bidder 7	As per RFP

			e participation, we request to change the clause to "**Should support an inbuilt /integrated Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.**"		
	Section 83 - WAF, Page 105, Clause 4.23	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	"Fake Search Engine Request" is not an industry standard term and can be a terminology used by some specific OEM restricting wide participation. Request you to change the clause to "**Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests/equivalent**"	Bidder 7	As per RFP

	Section 83 - WAF, Page 105, Clause 4.24	It should support scanning for malicious content in uploads along with File upload violations and support integration with APT solution to scan for zero day malwares.	Such integration will require the WAF and APT solution from the same OEM which restricts the leading WAF OEMs to participate in the tender as there is only one OEM having both WAF and APT Solution. Since, this clause is specific to a single OEM, request to relax the clause to "**It should support protection against Illegal File Upload/Download Volations. The Load Balancer, the WAF Module and the APT should be from different OEMs to strengthen the security posture.**"	Bidder 7	Please refer to corrigendum Point 9

	Section 83 - WAF, Page 106, Clause 9.1	Appliance should be able to terminate SSL	Since appliance has been asked to terminate SSL, sizing parameters are very important to qualify the hardware for the requirement. We request to change the clause to "**Appliance should be able to terminate SSL. The Appliance should support a minimum of 50,000 SSL TPS (RSA 2K Key) and 35,000 ECC TPS (ECDSA P256) from Day 1.**"	Bidder 7	As per RFP
	Section 83 - WAF, Page 106, Clause 9.2	Should Passively decrypt SSL	Passive SSL Decryption is an obsolete technology and the latest one is Active decryption. Hence, we request to change the clause to "**Should Actively/ Passively decrypt SSL**"	Bidder 7	As per RFP

	Section 83 - WAF, Page 106, Clause 11.1	The product must possess a Web Application Vulnerability Scanning capability built in.	As mentioned previously, some vendors have inbuilt Web Application Vulnerabilty scanner and some have their WAF and their Scanner integrate as and when needed. Hence, for wider participation, we request you to change the clause to "**The product must support Web Application Vulnerability Scanning capability built-in or via integration**"	Bidder 7	Please refer to corrigendum point 10
	Section 83 - WAF, Page 107, Clause 12.8	Should support and two Factor Authentication	Along with two factor authentication, it is critical to authenticate and allow only legitimate machines/endpoints to access the department's critical applications. Hence, we request to	Bidder 7	As per RFP

			change the clause to "**Should support and two Factor Authentication. The solution should have license upgrade feature on same appliance to support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access/authentication to critical resources.**"		
	Section 83 - WAF, Page 107, Clause 13.3	Should support multiple log formats such as CSV, Syslog, TXT, etc..	Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change the clause to "**Should support multiple log for**	Bidder 7	Please refer to corrigendum Point 11

				mats such as CSV/Syslog/TXT etc."		
	Section 83 - WAF, Page 107, Clause 13.5	Should support report formats in PDF, HTML, WORD, RTF, etc..		Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change the clause to "**Should support report formats in PDF/HTML/WORD/RTF etc.**"	Bidder 7	Please refer to corrigendum Point 12
1	-	-	**Since all Government department has opted e-bidding system for procurement and better transparancy. So, request you to please accept the e-bidding procure.**		Bidder 8	As per RFP
2	Pg no-7, Fact Sheet, Section -23	EMD- Bank Guarantee	Request you to please share your bank IFSC Code for BG preparation and verfication purpose.		Bidder 8	
3	Pg no- 26, Clause -13	Payment Schedule	Request you to give relaxation on this point as below: 1) Supply : 80% Payment release. 2) Comissioning : 1		Bidder 8	As per RFP

			5% Payment release. 3) Sign-off : 5% Payment release.			
4	Pg no- 43, Clause- 35.10	In case of bidders, other than the OEM, the bidder must have at least 10 qualified Engineers (minimum qualification diploma holder), on its roll, trained by the OEM of the quoted BOM items.	We wish to inform you that multiple OEM will be involved in single solution. Therefore, we reqeust you to clarify that engineer's capability and certifications required from all the OEM or we can provide Engineers capable of qualified diploma in any of field from the solution.		Bidder 8	The engineers shold cover major components
5	Pg no- 114, clause no- 36	The bidder should have experience in executing similar projects (procuring, supplying, commissioning and supporting servers/ storage) in Government/ PSU/ Banks/ BFSI sector in India with order value more than INR 10 crore	We request you to please give relaxation to bidders in respect of required experience by bidder i.e. similar projects of vlaue more than 10 Crore. This will enable more competitive bidding. Please allow bidder to provide similar Purchase order of value upto 2 Crore.		Bidder 8	As per RFP
6	Pg no- 114, clause no- 36	The bidder should have experience in procuring, supplying and commissioning the proposed infrastructure.	please clarify if bidder can use work orders of IT/ITES / server/storage/Security / Data Centre projects/software etc.		Bidder 8	As per RFP

7	83. Section WAF Page No. 104, 2.1	Should support 150,000 HTTP Transactions per second & atleast 90,000 HTTPS transactions per second.	The Sizing parameters mentioned w.r.t. HTTPS transactions per second is not inline with the Throughput requirement which is just 1 Gbps. Also we suggest to include the latest ECC cipher suite to be included to ensure that the application willl be compliant to TLS1.3. Hence we request to ammend this clause. **Suggested Clause:- Should support 150,000 HTTP Transactions per second & atleast 30,000 HTTPS transactions per second on RSA (2K) keys and 20K on ECC.**		Bidder 8	As per RFP
8	83. Section WAF 104 3.1	Should support 4 no.'s of 10/100/1000 interfaces with integerated/ external hardware bypass & 4 X 10 G SFP+SR ports	The WAF is a very critical security component so in any case traffic should not bypass the WAF security as the Back end Application will be exposed for attacks and can be compromised. Since the high Availability is already been asked in the Technical specification which will make sure that in case of primary device failure the secondary appliance will take over and Inspection of web tr		Bidder 8	As per RFP

			affic will not be co mpromised. Hence we request t o ammend this cla use. **Suggested Clause:-** Solution should su pport 8X10G SFP+ ports from day one scalable to 12X10G SFP+ ports to cater future requirement s.			
9	83. Section W AF 104 3.2	Should support 2TB of Stora ge space	As we understand t he Storage space r equirement mentio ned as 2TB should be for storing the L og data. Since the method of storing t he log data varies f rom OEM to OEM. Hence we would su ggest to mention t he exact requireme nt in terms of stori ng the log data and also its duration. **Suggested Clause:** The device should be able to store th e attack logs daily, weekly,Monthly,Q uaterly and Yearly. Also Administrator should be able to e xtract the logs for C ustom defined peri od/dates.		Bidder 8	As per RFP

10	83. Section WAF 105 4.1	The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode.	Device should be deployed in reverse proxy mode for better security coverage w.r.t OWASP top 10 and should be able to steer the application traffic if required which can be a challenge in Reverse proxy mode. Hence we suggest to ammend this clause. **Suggested Clause**:- The appliance should be able to perform in multiple modes of Deployment such as • Out-Of Path mode • Reverse proxy/Inline Policy Action • Block (Active) & Report (Passive) Policy Action • Report		Bidder 8	As per RFP
11	83. Section WAF 105 4.3	Should have a Web vulnerability Scanner to detect existing vulnerabilities in the protected web application	By using auto discovery mode the Web application firewall can scan the Application changes and patch them automatically for any vulnerability without any manual intervention using Auto-Discovery and Auto Policy generation which is fastest and very quick with minimal False positives. Hence we request to ammend this clause accordingly.		Bidder 8	As per RFP

			Suggested Clause:- Should have a Web vulnerability Scanner/Auto Discovery feature to detect and protect vulnerabilities in the protected web application with minimal false positives.			
12	83. Section WAF 105 4.7	WAF should support fail open in case of hardware failure	The WAF is a very critical security component so in any case traffic should not bypass the WAF security as the Back end Application will be exposed for attacks and can be compromised. Since the high Availability is already been asked in the Technical specification which will make sure that in case of primary device failure the secondary appliance will take over and Inspection of web traffic will not be compromised. Hence we request to remove this clause. **Suggested Clause:-** Remove this clause		Bidder 8	As per RFP

13	83. Section WAF Page No. 106 11.1	The product must possess a Web Application Vulnerability Scanning capability built in	By using auto discovery mode the Web application firewall can scan the Application changes and patch them automatically for any vulnerability without any manual intervention using Auto-Discovery and Auto Policy generation which is fastest and very quick with minimal False positives. Hence we request to ammend this clause accordingly. **Suggested Clause:-** The product must possess a Web Application Vulnerability Scanning capability/Auto discovery feature built in		Bidder 8	Please refer to corrigendum point 10
14	83. Section WAF Page No. 106 11.2	The Vulnerability scan should identify vulnerabilities such as xss, SQL Injection, Source code disclosure, Common web server vulnerabilities etc.	By using auto discovery mode the Web application firewall can scan the Application changes and patch them automatically for any vulnerability without any manual intervention using Auto-Discovery and Auto Policy generation which is fastest and very quick with minimal False positives. Hence we request to ammend this clause accordingly. **Suggested Clause:-** The Vulnerability scan/Auto discovery		Bidder 8	As per RFP

			feature should identify and patch the vulnerabilities such as xss, SQL Injection, Source code disclosure, Common web server vulnerabilities etc.			
15	83. Section WAF Page No. 106 11.3	Scan must be able to crawl the Web application	We suggest that WAF should be able to prevent the Crawlers from accessing the application. Crawlers consume resources on visited systems and often visit sites without approval. The WAF should be smart enough to sense the change automatically in backend application and patch the same without manual intervention. Hence we suggest to remove this clause. **Suggested Clause:**- Remove this clause.		Bidder 8	As per RFP

16	83. Section WAF Page No. 106 11.5	Should support scheduled scanning	The scanning should be an Ongoing process without manual intervention. Scheduling a scan can lead to Application compromise as nobody knows when an attack will be launched towards the web application. So it is suggested to place the WAF with discovery module on and continously monitoring every possbile change in application behaviour and block the attack traffic once identified as vulnerable. **Suggested Clause:-** Should support Continuous monitoring/scanning.		Bidder 8	As per RFP
17	83. Section WAF Page No. 106 11.6	Should support exclusions in scanning by the administrator	The scanning should be an Ongoing process without manual intervention. Scheduling a scan can lead to Application compromise as nobody knows when an attack will be launched towards the web application. So it is suggested to place the WAF with discovery module on and continously monitoring every possbile change in application behaviour and block the attack traffic once identified as vulnerable.		Bidder 8	As per RFP

			Suggested Clause:- Should support Continuous monitoring/manual scanning.			
18	New Clause Request	The system should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, and acceleration resources to provide complete separate environment from applications and management perspective.	**Suggested Clause :** Should be appliance based solution with purpose built hardware for high performance with ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) OS The proposed device should support upto 32 Virtual Instance		Bidder 8	As per RFP
19	New Clause Request	Include industry standard certification and references.	**Suggested Clause:** OEM should be present in Gartner Magic quadrant in the latest WAF report		Bidder 8	As per RFP

20	New Clause Request	The Web Application firewall should be able to integrate with Proposed DDoS solution at Perimeter so it can share the attack details using Messaging mechanism with DDoS Mitigation appliance at the perimeter to block the attack at perimeter and prevent it from entering the DC itself.	**Suggested Clause:-** The Web Application Firewall should be able integrate with proposed DDoS Mitigation Appliance at perimeter so it can share the attack details using Messaging mechanism with DDoS Mitigation appliance at the perimeter to block the attack at perimeter with DDoS Mitigator and prevent it from entering the DC itself.		Bidder 8	As per RFP
21	84. DDOS				Bidder 8	
22	84. DDoS Page No. 1071	The proposed solution should be appliance based solution	The DDoS mitigation device should be a high performance dedicated appliance it should not hold any IP on traffic ports. The device should be invisible in the network so that it cannot be targeted by any DDoS attack. **Suggested Clause:-** DDoS mitigation solution should be a dedicated appliance (not a part of Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Device).		Bidder 8	As per RFP

23	84. DDoS Page No. 107 4	Solution must support atleast 8X1G LAN and 8X1G WAN inerfaces	The current solution should be able to scale for 10 G network as well considering future requirements in perspective. For a DDoS Mitigation device which will placed at perimeter its highly recommended to go with SFP+ ports which gives the flexibility to adopt to 1G ports as well as 10 G ports as per the requirements. **Suggested Clause:-** Solution must support atleast 20X10G SFP+ ports.		Bidder 8	As per RFP
24	84. DDoS Page No. 107 10	System must be delivered as a rack mountable single-box solution	**Suggested Clause:** The Proposed DDoS Mitigation device should have 1U/2U form factor		Bidder 8	As per RFP
25	84. DDoS Page No. 107 14	Latency should be lower than 50 microseconds	Latency Factor vary from Packet size i.e. Higher the Packet Size; lesser the Latency. Majority of the Leading DDOS OEM's don't publish the Internal Testing reports wrt Latency viz-a-viz Packet Size. Exisiting clause is ambiguous, hence kindly delete or generalise this clause. **Suggested Clause:-** Latency should be l		Bidder 8	As per RFP

			ower than 100 micr oseconds			
26	New Clause R equest	Pre-Qualification criteria mu st be specified to ensure qu ality OEM's.	OEM should be pre sent in the Leader's quadrant for the la test Published Forr ester Report for DD oS Mitigation Solut ion. **Suggested Clause:-** OEM should be pre sent in the Leader's quadrant for the la test Published Forr ester Report for DD oS Mitigation Solut ion.		Bidder 8	As per RFP
27	New Clause R equest	The DDoS Mitigation Solutio n should be able to integrat e with Proposed WAF soluti on to provide precise mitiga tion under multivector Attac k scenerio	**Suggested Clause:-** The DDoS Mitigati on Appliance shoul d be able integrate with Proposed WA F solution.		Bidder 8	As per RFP
28	Load Balance r				Bidder 8	
29	85. Load Bala ncer Page No.110 1.6	Appliance should provide ful l ipv6 support and OEM sho uld be IPv6.org gold-certifie d. OEM should be listed ven dor for ipv6 phase-2 certific ation	Only Industry stand ard certification sh ould be considered . Hence we suggest to ammend this cla use. **Suggested Clause:-** Appliance should p rovide full ipv6 sup		Bidder 8	As per RFP

			port.OEM should be listed vendor for ipv6 phase-2 certification			
30	New Clause Request	Pre-Qualification criteria must be specified to ensure quality OEM's.	**Suggested Clause:** OEM should be present in Gartner's LEADER magic quadrant in the latest ADC report		Bidder 8	As per RFP
31	New Clause Request	The device should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, and acceleration resources to provide complete separate environment from applications and management perspective.	**Suggested Clause :** Should be appliance based solution with purpose built hardware for high performance with ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) OS The proposed device should support 5 vADC from day 1 scalable to 20 vADC on the same hardware.		Bidder 8	As per RFP

1	Section 85 - Load Balancer, Page 110, Clause 2.6	IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation	Along with IPv6 support for DNS 64/46, it is critical that the LLB supports advanced DNS functions to achieve critical Inbound Load Balancing features. We recommend to change the clause to "**IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation. It should also support advanced functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc..**"		Bidder 9	As per RFP
2	Section 85 - Load Balancer, Page 110, Clause 3.1	Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode.	Some vendors use proprietary protocols for achieving HA which makes it difficult to troubleshoot or seamlessly integrate with parrallel/inline devices. To maintain interoperability and integration, we request to change the clause to "**Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-acti**		Bidder 9	Please refer to corrigendum point 1

			ve & active standb y unit redundancy mode. The HA/Clu ster shall be achiev ed using Standard VRRP (RFC 2338) a nd no proprietary protocols shall be used for the same. "			
3	Section 85 - L oad Balancer, Page 110, Cla use 2.7	Domain name support for o utbound link selection for F QDN based load balancing.	Along with Link Loa d Balancing and sel ection of the outbo und link based on F QDN, the LLB shoul d also support forw ard proxy deploym ents to sanitize the outgoing requests. We request you to change the clause t o "**Domain name s upport for outbou nd link selection fo r FQDN based load balancing. The App liance should also support acting as a Webagent service to implement expli cit Forward proxy mode and to perfo rm DNS Caching** "		Bidder 9	As per RFP
4	Section 83 - WAF, Page 10 4, Clause 3.1	Should support 4 no's of 10 /100/1000 Interfaces with in tegrated / external hardwar e bypass & 4 x 10G SFP+ SR ports	In considering any solution, scalability is of utmost import ance. Hence, we re quest you to chang e the clause to "**Sh ould support 4 no' s of 10/100/1000 I nterfaces with inte grated / external h ardware bypass &**		Bidder 9	As per RFP

			4 x 10G SFP+ SR ports along with 2x40G QSFP+ Interfaces for future scalability"			
5	Section 83 - WAF, Page 104, Clause 3.2	Should support 2TB of Storage space	Since WAF will be frontending all the critical/protected applications, a lot of scanning and memory intensive functions shall be performed on the WAF. Hence, we request to add the minimum RAM/Memory criteria as well. Please change the clause to "**Should support 2TB of Storage space along with 64 GB RAM from Day 1.**"		Bidder 9	As per RFP
6	Section 83 - WAF, Page 105, Clause 4.3	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.	Each vendor caters to the Web vulnerability scanner in a different manner. Some OEMs have inbuilt capability and some vendors use separate Web Vulnerabily Scanners. Hence, to ensure wide participation, we request to change the clause to "**Should support an inbuilt/integrated Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.**"		Bidder 9	As per RFP

7	Section 83 - WAF, Page 105, Clause 4.23	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	"Fake Search Engine Request" is not an industry standard term and can be a terminology used by some specific OEM restricting wide participation. Request you to change the clause to "**Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests/ equivalent**"		Bidder 9	As per RFP
8	Section 83 - WAF, Page 105, Clause 4.24	It should support scanning for malicious content in uploads along with File upload violations and support integration with APT solution to scan for zero day malwares.	Such integration will require the WAF and APT solution from the same OEM which restricts the leading WAF OEMs to participate in the tender as there is only one OEM having both WAF and APT Solution. Since, this clause is specific to a single OEM, request to relax the clause to "**It should support protection against Illegal File Upload/Download Volations**"		Bidder 9	Please refer to corrigendum Point 9
9	Section 83 - WAF, Page 106, Clause 9.1	Appliance should be able to terminate SSL	Since appliance has been asked to terminate SSL, sizing parameters are very important to qualify the hardware for the requirement. We request to change the clause to "**Applicance should be able to terminate**		Bidder 9	As per RFP

			SSL. The Appliance should support a minimum of 50,000 SSL TPS (RSA 2K Key) and 35,000 ECC TPS (ECDSA P256) from Day 1."			
10	Section 83 - WAF, Page 106, Clause 9.2	Should Passively decrypt SSL	Passive SSL Decryption is an obsolete technology and the latest one is Active decryption. Hence, we request to change the clause to "**Should Actively/Passively decrypt SSL**"		Bidder 9	As per RFP
11	Section 83 - WAF, Page 106, Clause 11.1	The product must possess a Web Application Vulnerability Scanning capability built in.	As mentioned previously, some vendors have inbuilt Web Application Vulnerabilty scanner and some have their WAF and their Scanner integrate as and when needed. Hence, for wider participation, we request you to change the clause to "**The product must support Web Application Vulnerability Scanning capability built-in or via integration**"		Bidder 9	Please refer to corrigendum point 10

12	Section 83 - WAF, Page 107, Clause 12.8	Should support and two Factor Authentication	Along with two factor authentication, it is critical to authenticate and allow only legitimate machines/endpoints to access the department's critical applications. Hence, we request to change the clause to "**Should support and two Factor Authentication. The solution should have license upgrade feature on same appliance to support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access/authentication to critical resources.**"		Bidder 9	As per RFP
13	Section 83 - WAF, Page 107, Clause 13.3	Should support multiple log formats such as CSV, Syslog, TXT, etc..	Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change the clause to "**Should support multiple log formats such as CSV/Syslog/TXT etc.**."		Bidder 9	Please refer to corrigendum Point 11
14	Section 83 - WAF, Page 107, Clause 13.5	Should support report formats in PDF, HTML, WORD, RTF, etc..	Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change th		Bidder 9	Please refer to corrigendum Point 12

			e clause to "**Should support report for mats in PDF/HTML /WORD/RTF etc.**"			
15	Section 84 - DDoS, Page no. 107 - Clause no. 4	Solution must support at lea st 8 x 1G LAN & 8 x 1G WAN interfaces	According to the RFP, the throughput asked is 6 Gbps and correspondingly, this clause asks for much higher number of interfaces. Request to change the clause to "**Solution must support at least 2 X 1G LAN & 2 X 1G WAN Interfaces and 2 X 10 GBE SFP+ Ports for future scalability**"		Bidder 9	As per RFP
16	Section 84 - DDoS, Page no. 107 - Clause no. 5	Solution must at least suppo rt 6Gbps of Enterprise Mix traffic	Since most of the traffic is SSL based and the Anti-DDoS Device needs to be SSL aware and ready, it is imperative to size the device with SSL/ECC Parameters as well. Hence, we request to change the clause to "**Solution must at least support 6 Gbps of Enterprise mix Traffic. The appliance should support a minimum SSL TPS (RSA 2K) of 20,000 and ECC TPS (ECDSA P256) of 14,000 from Day 1**"		Bidder 9	As per RFP

17	Section 84 - DDoS, Page no. 107 - Clause no. 8	The device should support high availability	As mentioned earlier, to ensure interoperability and easy troubleshooting process, the device should use industry standard protocols for HA. Hence, we request to change the clause to "**The Device should support high availability. The HA/Clustering should be based on Standard VRRP (RFC 2338) and no proprietary protocols shall be used**"		Bidder 9	As per RFP
18	Section 84 - DDoS, Page no. 108 - Clause no. 18	The system must have an updated threat feed that describes new malicious traffic (botnets, phishing, etc...).	Every OEM has a different way of dealing with new and updated threat vectors. Some do it via threat feed and some vendors use a complete behavorial approach when detecting and mitigating threats. Hence, we request to relax the clause to "**The system must have an updated threat feed/On device Behaviour detection engine that describes new malicious traffic (Botnets, phishing, etc...)**"		Bidder 9	As per RFP
19	Section 84 - DDoS, Page no. 109 - Clause no. 42	It should be possible to block Geographical Locations to prevent flooding attacks from a particular country	This fuctionality can be either achieved using geography database or by using identifying geographies in the form of IP Ranges. Hence, we request relax		Bidder 9	As per RFP

			ing the clause to "**It should be possible to block Geographical locations/Source IP Address/Source IP Ranges to prevent flooding attacks from a particular country**"			
20	Section 84 - DDoS, Page no. 109 - Clause no. 43	DDoS Appliance should receive a continuous update feed of Malicious Sources categorize as phishing, botnet etc	Every OEM has a different way of dealing with new and updated threat vectors. Some do it via threat feed and some vendors use a complete behavorial approach when detecting and mitigating threats. Hence, we request to relax the clause to "**DDoS Appliance should receive a continous update feed or should have an on-device behaviour engine of Malicious sources which can be categorized as phishing, botnet etc ...**"		Bidder 9	As per RFP
21	Section 81- SIEM,point-1,pg-112	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.	SIEM AND PACKET SHOULD BE TREATED AS SEORATE SOLUTIONS AND MUST INTEGRATE WITH EACH OTHER. PACKET CAPTURE IS VERY SPECIFIC REQUIREMENT AND HAVE DIFFERENT USE CASES THAT OF SIEM. THIS POINT IS PROPERITORY TO AN OEM WHO DOES UNIFIED SIEM WITH P	NEXT GENERATION PLATFORM MUST INTEGRATE WITH SPECILAISED PACKET CAPTURE SOLUTIONS LIKE NIKSUN, SOLERA, EXINDA. MUST BE THREE TIER PHYSICALLY SEGR	Bidder 9	As per RFP

			ACKET BUT DOES NOT GOVE PROPER OR COMPLTETE SOLUTION	EGATED ARCHITEURE CONSISTING OF LOG COLLECTION, LOG MANAGEMENT AND LOG CORRELATION ON PURPOSE BUILT APPLIANCE/HARDWARE WITH ADVANCED CAPABILITIES LIKE THREAT INTELLIGENCE, USER ANALYTICS, APPLICATION ANALYTICS		
22	Section 81- SIEM,point-2,pg-112	SIEM for Logs and deep packet inspection should be from same OEM.	SIEM AND PACKET SHOULD BE TREATED AS SEORATE SOLUTIONS AND MUST INTEGRATE WITH EACH OTHER. PACKET CAPTURE IS VERY SPECIFIC REQUIREMENT AND HAVE DIFFERENT USE CASES THAT OF SIEM. THIS POINT IS PROPERITORY TO AN OEM WHO DOES UNIFIED SIEM WITH PACKET BUT DOES NOT GOVE PROPER OR COMPLTETE SOLUTION	SIEM AND PACKET SOLUTION MUST COME FROM DIFFERENT OEM , SPECIALISING IN EACH AND MUST INTEGRATE FOR USE CASES TO BE DRIVEN	Bidder 9	As per RFP

23	Section 81- SIEM,point-8,pg-112	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.	LOGS ARE HIGHLY SENSITIVE AND ARE IN NUMBERS, HENCE ITS IMPORTANT TO PROTECT THEM AS WELL AS AGGREGATE AND COMPRESS.	LOGS MUST BE COMPRESSED ATLEAST 90%, MUST BE AGGREGATED AND FILTERED AT COLLECTOR LEVEL AND INGPROTECTED BY de-identify logs right at source through format peserving Encryption which should e NIST certified . The Solution should proide Field level encryption and decryption and based on roles the fileds should be decrypted based on roles . The Encryption algorith should make sure the Logs size is not increased and provides protection of Critical logs in rest, move and in use	Bidder 9	As per RFP

24	Section 81- SIEM,point-9,pg-112	A single log appliance should support minimum 10,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.	LOGS ARE IN GB/DAY AND MUST NOT BE MIXED WITH PACKETS AS BOTH ARE DIFFERENT	LOG MANAGEMENT APPLIANCE MUST BE 250GB/DAY ON PURPOSE BUILT APPLIANCE HAVING AT LEAST 128 GB RAM AND 12 TB OF INBUILT STORAGE PACKET APPLIANCE MUST BE SEPRATE AS PER NETWORK REQUIREMENT	Bidder 9	As per RFP
25	Section 81- SIEM,point-10,pg-112	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 20,000 EPS.	COORELATION IS ALWAYS FOR SECURITY THREATS BASED ON USE CASES HENCE LESSER AS COMPARED TO LOG MANAGEMENT WHERE ALL LOGS ARE CONSOLIDATED	CORRELATION LAYER MUST BE 5000 SUSTAINED/20000 PEAK EPS ON APPLIANCE WITH MINIMUM 192 GB RAM FOR OPTIMAL PERFORMANCE AND 1 MONTH OF ONLINE CORRELATED LOG STORAGE	Bidder 9	As per RFP
26	Section 81- SIEM,point-14,pg-113	Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.	COVERED ABOVE	CAN BE REMOVED AS COVERED ABOVE	Bidder 9	As per RFP
27	Section 81- SIEM,point-18,pg-113	Should be able to filter the captured packets based on layer- 2 to layer-7 header info	PROPERITORY TO OEM	SHOULD BE ABLE TO FILTER AND C	Bidder 9	As per RFP

		rmation.		APTURE LOGS BASED ON LAYER - 2 TO 7 HEADER INFORMATION		
28	Section 81- SIEM,point-19, pg-113	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.	PROPERITORY TO OEM	REQUEST TO BE REMOVED	Bidder 9	As per RFP
29	Section 81- SIEM,point-20, pg-113	The proposed solution must be able to provide the complete platform to perform Network forensics solution	LOG FORECSICS, WE ARE TALKING OF SIEM AND NOT NBAD. THESE POINTS SHOULD BE SEPRATE IN NBAD	THE PROPOSED SOLUTION MUST BE ABLE TO PROVIDE COMPLETE PLATFORM TO PERFOM LOG FORENSICS AND ANLYTICS	Bidder 9	As per RFP
30	Section 81- SIEM,point-21, pg-113	The solution must be able to detect malicious payload in network traffic	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 9	As per RFP
31	Section 81- SIEM,point-22, pg-113	• Detect and reconstruct files back to its original type	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 9	As per RFP
32	Section 81- SIEM,point-23, pg-113	• Detect hidden or embedded files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 9	As per RFP
33	Section 81- SIEM,point-24, pg-113	• Detect and flag out renamed files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 9	As per RFP
34	Section 81- SIEM,point-25, pg-113	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure .	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 9	As per RFP
35	NEW CLAUSE	NEW POINT SUGGESTION	SIEM solution must integarte with all key IT infrastructire of Smart city and must have integartion with applications to pull security logs like SQL injection, XSS through agents.		Bidder 9	As per RFP

			Even if aplication does not natively generate logs it must have a provision to pull logs and must not depend only on WAF for those logs.			
36	NEW CLAUSE	NEW POINT SUGGESTION	Proposed SIEM tool must be in existence for past 7 years atelast and should have evolved . OEM must not have declared its SIEM solution as end of life at anytime in last 7 years		Bidder 9	As per RFP
	Section 85 - Load Balancer, Page 110, Clause 2.6	IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation	Along with IPv6 support for DNS 64/46, it is critical that the LLB supports advanced DNS functions to achieve critical Inbound Load Balancing features. We recommend to change the clause to "**IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation. It should also support advanced functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc..**"		Bidder 10	As per RFP

	Section 85 - Load Balancer, Page 110, Clause 3.1	Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode.	Some vendors use proprietary protocols for achieving HA which makes it difficult to troubleshoot or seamlessly integrate with parrallel/inline devices. To maintain interoperability and integration, we request to change the clause to "**Should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode. The HA/Cluster shall be achieved using Standard VRRP (RFC 2338) and no proprietary protocols shall be used for the same.** "		Bidder 10	Please refer to corrigendum point 1
	Section 85 - Load Balancer, Page 110, Clause 2.7	Domain name support for outbound link selection for FQDN based load balancing.	Along with Link Load Balancing and selection of the outbound link based on FQDN, the LLB should also support forward proxy deployments to sanitize the outgoing requests. We request you to change the clause to "**Domain name support for outbound link selection for FQDN based load balancing. The Appliance should also support acting as a Webagent service**		Bidder 10	As per RFP

			to implement explicit Forward proxy mode and to perform DNS Caching "			
	Section 83 - WAF, Page 104, Clause 3.1	Should support 4 no's of 10/100/1000 Interfaces with integrated / external hardware bypass & 4 x 10G SFP+ SR ports	In considering any solution, scalability is of utmost importance. Hence, we request you to change the clause to "**Should support 4 no's of 10/100/1000 Interfaces with integrated / external hardware bypass & 4 x 10G SFP+ SR ports along with 2x40G QSFP+ Interfaces for future scalability**"		Bidder 10	As per RFP
	Section 83 - WAF, Page 104, Clause 3.2	Should support 2TB of Storage space	Since WAF will be frontending all the critical/protected applications, a lot of scanning and memory intensive functions shall be performed on the WAF. Hence, we request to add the minimum RAM/Memory criteria as well. Please change the clause to "**Should support 2TB of Storage space along with 64 GB RAM from Day 1.**"		Bidder 10	As per RFP

	Section 83 - WAF, Page 105, Clause 4.3	Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.	Each vendor cater to the Web vulnerability scanner in a different manner. Some OEMs have inbuilt capability and some vendors use separate Web Vulnerabily Scanners. Hence, to ensure wide participation, we request to change the clause to "**Should support an inbuilt/integrated Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.**"		Bidder 10	As per RFP
	Section 83 - WAF, Page 105, Clause 4.23	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	"Fake Search Engine Request" is not an industry standard term and can be a terminology used by some specific OEM restricting wide participation. Request you to change the clause to "**Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests/ equivalent**"		Bidder 10	As per RFP
	Section 83 - WAF, Page 105, Clause 4.24	It should support scanning for malicious content in uploads along with File upload violations and support integration with APT solution to scan for zero day malwares.	Such integration will require the WAF and APT solution from the same OEM which restricts the leading WAF OEMs to participate in the tender as there is only one OEM having both WAF and A		Bidder 10	Please refer to corrigendum Point 9

			PT Solution. Since, this clause is specific to a single OEM, request to relax the clause to "**It should support protection against Illegal File Upload/Download Volations**"			
	Section 83 - WAF, Page 106, Clause 9.1	Appliance should be able to terminate SSL	Since appliance has been asked to terminate SSL, sizing parameters are very important to qualify the hardware for the requirement. We request to change the clause to "**Applicance should be able to terminate SSL. The Appliance should support a minimum of 50,000 SSL TPS (RSA 2K Key) and 35,000 ECC TPS (ECDSA P256) from Day 1.**"		Bidder 10	As per RFP
	Section 83 - WAF, Page 106, Clause 9.2	Should Passively decrypt SSL	Passive SSL Decryption is an obsolete technology and the latest one is Active decryption. Hence, we request to change the clause to "**Should Actively/Passively decrypt SSL**"		Bidder 10	As per RFP
	Section 83 - WAF, Page 106, Clause 11.1	The product must possess a Web Application Vulnerability Scanning capability built in.	As mentioned previously, some vendors have inbuilt Web Application Vulnerabilty scanner and some have their WAF and their Scanner integrate as and when needed. Hence, for wider participation, we request		Bidder 10	Please refer to corrigendum point 10

			you to change the clause to "**The product must support Web Application Vulnerability Scanning capability built-in or via integration**"			
	Section 83 - WAF, Page 107, Clause 12.8	Should support and two Factor Authentication	Along with two factor authentication, it is critical to authenticate and allow only legitimate machines/endpoints to access the department's critical applications. Hence, we request to change the clause to "**Should support and two Factor Authentication. The solution should have license upgrade feature on same appliance to support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access/authentication to critical resources.**"		Bidder 10	As per RFP
	Section 83 - WAF, Page 107, Clause 13.3	Should support multiple log formats such as CSV, Syslog, TXT, etc..	Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change the clause to "**Should support multiple log formats such as C**		Bidder 10	Please refer to corrigendum Point 11

			SV/Syslog/TXT etc. ."			
	Section 83 - WAF, Page 107, Clause 13.5	Should support report formats in PDF, HTML, WORD, RTF, etc..	Different OEMs may support different log/report formats and hence to ensure wider participants in the RFP, we request to change the clause to "**Should support report formats in PDF/HTML/WORD/RTF etc.**"		Bidder 10	Please refer to corrigendum Point 12
	Section 84 - DDoS, Page no. 107 - Clause no. 4	Solution must support at least 8 x 1G LAN & 8 x 1G WAN interfaces	According to the RFP, the throughput asked is 6 Gbps and correspondingly, this clause asks for much higher number of interfaces. Request to change the clause to "**Solution must support at least 2 X 1G LAN & 2 X 1G WAN Interfaces and 2 X 10 GBE SFP+ Ports for future scalability**"		Bidder 10	As per RFP
	Section 84 - DDoS, Page no. 107 - Clause no. 5	Solution must at least support 6Gbps of Enterprise Mix traffic	Since most of the traffic is SSL based and the Anti-DDoS Device needs to be SSL aware and ready, it is imperative to size the device with SSL/ECC Parameters as well. Hence, we request to change the clause to "**Solution must at least support 6 Gbps of Enterprise mix Traffic. The appliance should support a**		Bidder 10	As per RFP

			minimum SSL TPS (RSA 2K) of 20,000 and ECC TPS (ECDS A P256) of 14,000 f rom Day 1"			
	Section 84 - D DoS, Page no. 107 - Clause no. 8	The device should support h igh availability	As mentioned earli er, to ensure intero perability and easy troubleshooting pr ocess, the device s hould use industry standard protocols for HA. Hence, we r equest to change t he clause to "**The D evice should suppo rt high availability. The HA/Clustering should be based o n Standard VRRP (RFC 2338) and no proprietary protoc ols shall be used**"		Bidder 10	As per RFP
	Section 84 - D DoS, Page no. 108 - Clause no. 18	The system must have an up dated threat feed that descr ibes new malicious traffic (b otnets, phishing, etc...).	Every OEM has a di fferent way of deali ng with new and u pdated threat vect ors. Some do it via threat feed and so me vendors use a c omplete behavorial approach when det ecting and mitigati ng threats. Hence, we request to relax the clause to "**The system must have an updated threat feed/On device Be haviour detection engine that descri bes new malicious**		Bidder 10	As per RFP

			traffic (Botnets, phishing, etc...)"			
	Section 84 - DDoS, Page no. 109 - Clause no. 42	It should be possible to block Geographical Locations to prevent flooding attacks from a particular country	This fuctionality can be either achieved using geography database or by using identifying geographies in the form of IP Ranges. Hence, we request relaxing the clause to "**It should be possible to block Geographical locations/Source IP Address/Source IP Ranges to prevent flooding attacks from a particular country**"		Bidder 10	As per RFP
	Section 84 - DDoS, Page no. 109 - Clause no. 43	DDoS Appliance should receive a continuous update feed of Malicious Sources categorize as phishing, botnet etc	Every OEM has a different way of dealing with new and updated threat vectors. Some do it via threat feed and some vendors use a complete behavorial approach when detecting and mitigating threats. Hence, we request to relax the clause to "**DDoS Appliance should receive a continous update feed or should have an on-device behaviour engine of Malicious sources which can b**		Bidder 10	As per RFP

			e categorized as p hishing, botnet etc ..."			
	Section 81- SI EM,point-1,p g-112	Next generation platform sh ould encompass log, packet and end point data with add ed context and threat Intelli gence. Should provide comp lete network visibility throu gh deep packet inspection hi gh speed packet capture an d analysis.	SIEM AND PACKET SHOULD BE TREAT ED AS SEORATE SO LUTIONS AND MUS T INTEGRATE WITH EACH OTHER. PACK ET CAPTURE IS VER Y SPECIFIC REQUIR EMENT AND HAVE DIFFERENT USE CA SES THAT OF SIEM. THIS POINT IS PRO PERITORY TO AN O EM WHO DOES UN IFIED SIEM WITH P ACKET BUT DOES N OT GOVE PROPER OR COMPLTETE SO LUTION	NEXT GENE RATION PL ATFORM M UST INTEG RATE WITH SPECILAISE D PACKET C APTURE SO LUTIONS LI KE NIKSUN, SOLERA, EX INDA. MUS T BE THREE TIER PHYSI CALLY SEGR EGATED AR CHITEURE CONSISTIN G OF LOG C OLLECTION , LOG MAN AGEMENT AND LOG C ORRELATIO N ON PURP OSE BUILT APPLIANCE /HARDWAR E WITH AD VANCED CA PABILITIES LIKE THREA T INTELLIG ENCE, USER ANALYTICS, APPLICATI	Bidder 10	As per RFP

				ON ANALYTICS		
	Section 81- SIEM,point-2,pg-112	SIEM for Logs and deep packet inspection should be from same OEM.	SIEM AND PACKET SHOULD BE TREATED AS SEORATE SOLUTIONS AND MUST INTEGRATE WITH EACH OTHER. PACKET CAPTURE IS VERY SPECIFIC REQUIREMENT AND HAVE DIFFERENT USE CASES THAT OF SIEM. THIS POINT IS PROPERITORY TO AN OEM WHO DOES UNIFIED SIEM WITH PACKET BUT DOES NOT GOVE PROPER OR COMPLTETE SOLUTION	SIEM AND PACKET SOLUTION MUST COME FROM DIFFERENT OEM , SPECIALISING IN EACH AND MUST INTEGRATE FOR USE CASES TO BE DRIVEN	Bidder 10	As per RFP

	Section 81- SIEM,point-8,pg-112	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.	LOGS ARE HIGHLY SENSITIVE AND ARE IN NUMBERS, HENCE ITS IMPORTANT TO PROTECT THEM AS WELL AS AGGREGATE AND COMPRESS.	LOGS MUST BE COMPRESSED ATLEAST 90%, MUST BE AGGREGATED AND FILTERED AT COLLECTOR LEVEL AND INGPROTECTED BY de-identify logs right at source through format peserving Encryption which should e NIST certified . The Solution should proide Field level encryption and decryption and based on roles the fileds should be decrypted based on roles . The Encryption algorith should make sure the Logs size is not increased and provides protection of Critical logs in rest, move and in use	Bidder 10	As per RFP

	Section 81- SIEM,point-9,pg-112	A single log appliance should support minimum 10,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.	LOGS ARE IN GB/DAY AND MUST NOT BE MIXED WITH PACKETS AS BOTH ARE DIFFERENT	LOG MANAGEMENT APPLIANCE MUST BE 250GB/DAY ON PURPOSE BUILT APPLIANCE HAVING AT LEAST 128 GB RAM AND 12 TB OF INBUILT STORAGE PACKET APPLIANCE MUST BE SEPRATE AS PER NETWORK REQUIREMENT	Bidder 10	As per RFP
	Section 81- SIEM,point-10,pg-112	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 20,000 EPS.	COORELATION IS ALWAYS FOR SECURITY THREATS BASED ON USE CASES HENCE LESSER AS COMPARED TO LOG MANAGEMENT WHERE ALL LOGS ARE CONSOLIDATED	CORRELATION LAYER MUST BE 5000 SUSTAINED/20000 PEAK EPS ON APPLIANCE WITH MINIMUM 192 GB RAM FOR OPTIMAL PERFORMANCE AND 1 MONTH OF ONLINE CORRELATED LOG STORAGE	Bidder 10	As per RFP
	Section 81- SIEM,point-14,pg-113	Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.	COVERED ABOVE	CAN BE REMOVED AS COVERED ABOVE	Bidder 10	As per RFP
	Section 81- SIEM,point-18,pg-113	Should be able to filter the captured packets based on layer- 2 to layer-7 header info	PROPERITORY TO OEM	SHOULD BE ABLE TO FILTER AND C	Bidder 10	As per RFP

		rmation.		APTURE LOGS BASED ON LAYER - 2 TO 7 HEADER INFORMATION		
	Section 81- SIEM,point-19, pg-113	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.	PROPERITORY TO OEM	REQUEST TO BE REMOVED	Bidder 10	As per RFP
	Section 81- SIEM,point-20, pg-113	The proposed solution must be able to provide the complete platform to perform Network forensics solution	LOG FORECSICS, WE ARE TALKING OF SIEM AND NOT NBAD. THESE POINTS SHOULD BE SEPRATE IN NBAD	THE PROPOSED SOLUTION MUST BE ABLE TO PROVIDE COMPLETE PLATFORM TO PERFOM LOG FORENSICS AND ANLYTICS	Bidder 10	As per RFP
	Section 81- SIEM,point-21, pg-113	The solution must be able to detect malicious payload in network traffic	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 10	As per RFP
	Section 81- SIEM,point-22, pg-113	• Detect and reconstruct files back to its original type	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 10	As per RFP
	Section 81- SIEM,point-23, pg-113	• Detect hidden or embedded files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 10	As per RFP
	Section 81- SIEM,point-24, pg-113	• Detect and flag out renamed files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 10	As per RFP
	Section 81- SIEM,point-25, pg-113	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure .	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 10	As per RFP
	NEW CLAUSE	NEW POINT SUGGESTION	SIEM solution must integarte with all key IT infrastructire of Smart city and must have integartion with applications to pull security logs like SQL injection, XSS through agents.		Bidder 10	As per RFP

			Even if aplication does not natively generate logs it must have a provision to pull logs and must not depend only on WAF for those logs.			
	NEW CLAUSE	NEW POINT SUGGESTION	Proposed SIEM tool must be in existence for past 7 years atelast and should have evolved . OEM must not have declared its SIEM solution as end of life at anytime in last 7 years		Bidder 10	As per RFP
1	Section 81- SIEM,point-1,pg-112	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.	SIEM AND PACKET SHOULD BE TREATED AS SEPRATE SOLUTIONS AND MUST INTEGRATE WITH EACH OTHER. PACKET CAPTURE IS VERY SPECIFIC REQUIREMENT AND HAVE DIFFERENT USE CASES THAT OF SIEM.THIS POINT IS PROPERITORY TO AN OEM WHO DOES UNIFIED SIEM WITH PACKET BUT DOES NOT GOVE PROPER OR COMPLTETE SOLUTION	NEXT GENERATION PLATFORM MUST INTEGRATE WITH SPECILAISED PACKET CAPTURE SOLUTIONS LIKE NIKSUN, SOLERA, EXINDA. MUST BE THREE TIER PHYSICALLY SEGREGATED ARCHITEURE CONSISTING OF LOG COLLECTION, LOG MANAGEMENT AND LOG CORRELATION ON PURPOSE BUILT APPLIANCE/HARDWARE WITH ADVANCED CA	Bidder 11	As per RFP

				PABILITIES LIKE THREAT INTELLIGENCE, USER ANALYTICS, APPLICATION ANALYTICS		
2	Section 81- SIEM,point-2,pg-112	SIEM for Logs and deep packet inspection should be from same OEM.	SIEM AND PACKET SHOULD BE TREATED AS SEORATE SOLUTIONS AND MUST INTEGRATE WITH EACH OTHER. PACKET CAPTURE IS VERY SPECIFIC REQUIREMENT AND HAVE DIFFERENT USE CASES THAT OF SIEM. THIS POINT IS PROPERITORY TO AN OEM WHO DOES UNIFIED SIEM WITH PACKET BUT DOES NOT GOVE PROPER OR COMPLTETE SOLUTION	SIEM AND PACKET SOLUTION MUST COME FROM DIFFERENT OEM , SPECIALISING IN EACH AND MUST INTEGRATE FOR USE CASES TO BE DRIVEN	Bidder 11	As per RFP

3	Section 81- SIEM,point-8,pg-112	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.	LOGS ARE HIGHLY SENSITIVE AND ARE IN NUMBERS, HENCE ITS IMPORTANT TO PROTECT THEM AS WELL AS AGGREGATE AND COMPRESS.	LOGS MUST BE COMPRESSED ATLEAST 90%, MUST BE AGGREGATED AND FILTERED AT COLLECTOR LEVEL AND INGPROTECTED BY de-identify logs right at source through format peserving Encryption which should e NIST certified . The Solution should proide Field level encryption and decryption and based on roles the fileds should be decrypted based on roles . The Encryption algorith should make sure the Logs size is not increased and provides protection of Critical logs in rest, move and in use	Bidder 11	As per RFP

4	Section 81- SIEM,point-9,pg-112	A single log appliance should support minimum 10,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.	LOGS ARE IN GB/DAY AND MUST NOT BE MIXED WITH PACKETS AS BOTH ARE DIFFERENT	LOG MANAGEMENT APPLIANCE MUST BE 250GB/DAY ON PURPOSE BUILT APPLIANCE HAVING AT LEAST 128 GB RAM AND 12 TB OF INBUILT STORAGE PACKET APPLIANCE MUST BE SEPRATE AS PER NETWORK REQUIREMENT	Bidder 11	As per RFP
5	Section 81- SIEM,point-10,pg-112	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 20,000 EPS.	COORELATION IS ALWAYS FOR SECURITY THREATS BASED ON USE CASES HENCE LESSER AS COMPARED TO LOG MANAGEMENT WHERE ALL LOGS ARE CONSOLIDATED	CORRELATION LAYER MUST BE 5000 SUSTAINED/20000 PEAK EPS ON APPLIANCE WITH MINIMUM 192 GB RAM FOR OPTIMAL PERFORMANCE AND 1 MONTH OF ONLINE CORRELATED LOG STORAGE	Bidder 11	As per RFP
6	Section 81- SIEM,point-14,pg-113	Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.	COVERED ABOVE	CAN BE REMOVED AS COVERED ABOVE	Bidder 11	As per RFP
7	Section 81- SIEM,point-18,pg-113	Should be able to filter the captured packets based on layer- 2 to layer-7 header info	PROPERITORY TO OEM	SHOULD BE ABLE TO FILTER AND C	Bidder 11	As per RFP

		rmation.		APTURE LOGS BASED ON LAYER - 2 TO 7 HEADER INFORMATION		
8	Section 81- SIEM,point-19, pg-113	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.	PROPERITORY TO OEM	REQUEST TO BE REMOVED	Bidder 11	As per RFP
9	Section 81- SIEM,point-20, pg-113	The proposed solution must be able to provide the complete platform to perform Network forensics solution	LOG FORECSICS, WE ARE TALKING OF SIEM AND NOT NBAD. THESE POINTS SHOULD BE SEPRATE IN NBAD	THE PROPOSED SOLUTION MUST BE ABLE TO PROVIDE COMPLETE PLATFORM TO PERFOM LOG FORENSICS AND ANLYTICS	Bidder 11	As per RFP
10	Section 81- SIEM,point-21, pg-113	The solution must be able to detect malicious payload in network traffic	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 11	As per RFP
11	Section 81- SIEM,point-22, pg-113	• Detect and reconstruct files back to its original type	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 11	As per RFP
12	Section 81- SIEM,point-23, pg-113	• Detect hidden or embedded files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 11	As per RFP
13	Section 81- SIEM,point-24, pg-113	• Detect and flag out renamed files	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 11	As per RFP
14	Section 81- SIEM,point-25, pg-113	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure .	TO BE PART OF NBAD	REQUEST TO BE REMOVED	Bidder 11	As per RFP
15	NEW CLAUSE	NEW POINT SUGGESTION	SIEM solution must integarte with all key IT infrastructire of Smart city and must have integartion with applications to pull security logs like SQL injection, XSS through agents.		Bidder 11	As per RFP

			Even if aplication d oes not natively ge nerate logs it must have a provision to pull logs and must not depend only on WAF for those logs.			
16	NEW CLAUSE	NEW POINT SUGGESTION	Proposed SIEM too l must be in existen ce for past 7 years atelast and should have evolved . OE M must not have d eclared its SIEM sol ution as end of life at anytime in last 7 years		Bidder 11	As per RFP
1	83. Section W AF Page No. 104, 2.1	Should support 150,000 HTT P Transactions per second & atleast 90,000 HTTPS transa ctions per second.	The Sizing paramet ers mentioned w.r. t. HTTPS transactio ns per second is no t inline with the Th roughput requirem ent which is just 1 Gbps. Also we sug gest to include the latest ECC cipher s uite to be included to ensure that the application willl be compliant to TLS1. 3. Hence we request t o ammend this cla use. **Suggested Clause:- Should support 15 0,000 HTTP Transa ctions per second & atleast 30,000 H TTPS transactions per second on RSA (2K) keys and 20K on ECC.**		Bidder 12	As per RFP

2	83. Section WAF 104 3.1	Should support 4 no.'s of 10/100/1000 interfaces with integerated/ external hardware bypass & 4 X 10 G SFP+SR ports	The WAF is a very critical security component so in any case traffic should not bypass the WAF security as the Back end Application will be exposed for attacks and can be compromised. Since the high Availability is already been asked in the Technical specification which will make sure that in case of primary device failure the secondary appliance will take over and Inspection of web traffic will not be compromised. Hence we request to ammend this clause. **Suggested Clause:-** Solution should support 8X10G SFP+ ports from day one scalable to 12X10G SFP+ ports to cater future requirements.		Bidder 12	As per RFP

3	83. Section WAF 104 3.2	Should support 2TB of Storage space	As we understand the Storage space requirement mentioned as 2TB should be for storing the Log data. Since the method of storing the log data varies from OEM to OEM. Hence we would suggest to mention the exact requirement in terms of storing the log data and also its duration. **Suggested Clause:** The device should be able to store the attack logs daily, weekly,Monthly,Quaterly and Yearly. Also Administrator should be able to extract the logs for Custom defined period/dates.		Bidder 12	As per RFP
4	83. Section WAF 105 4.1	The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode.	Device should be deployed in reverse proxy mode for better security coverage w.r.t OWASP top 10 and should be able to steer the application traffic if required which can be a challenge in Reverse proxy mode. Hence we suggest to ammend this clause. **Suggested Clause**:- The appliance should be able to perform in multiple modes of Deployment su		Bidder 12	As per RFP

			ch as • Out-Of Path mod e • Reverse proxy/Inl ine Policy Action • Block (Active) & R eport (Passive) Policy Action • Report			
5	83. Section W AF 105 4.3	Should have a Web vulnerab ility Scanner to detect existi ng vulnerabilities in the prot ected web application	By using auto disco very mode the We b application firew all can scan the Ap plication changes a nd patch them aut omatically for any v ulnerability withou t any manual interv ention using Auto-Discovery and Auto Policy generation which is fastest an d very quick with m inimal False positiv es. Hence we requ est to ammend this clause accordingly. **Suggested Clause:-** Should have a Web vulnerability Scann er/Auto Discovery f eature to detect an d protect vulnerabi lities in the protect ed web application with minimal false positives.		Bidder 12	As per RFP

6	83. Section WAF 105 4.7	WAF should support fail open in case of hardware failure	The WAF is a very critical security component so in any case traffic should not bypass the WAF security as the Back end Application will be exposed for attacks and can be compromised. Since the high Availability is already been asked in the Technical specification which will make sure that in case of primary device failure the secondary appliance will take over and Inspection of web traffic will not be compromised. Hence we request to remove this clause. **Suggested Clause:-** Remove this clause		Bidder 12	As per RFP
7	83. Section WAF Page No. 106 11.1	The product must possess a Web Application Vulnerability Scanning capability built in	By using auto discovery mode the Web application firewall can scan the Application changes and patch them automatically for any vulnerability without any manual intervention using Auto-Discovery and Auto Policy generation which is fastest and very quick with minimal False positives. Hence we request to ammend this clause accordingly.		Bidder 12	Please refer to corrigendum point 10

			Suggested Clause:- The product must possess a Web Application Vulnerability Scanning capability/Auto discovery feature built in			
8	83. Section WAF Page No. 106 11.2	The Vulnerability scan should identify vulnerabilities such as xss, SQL Injection, Source code disclosure, Common web server vulnerabilities etc.	By using auto discovery mode the Web application firewall can scan the Application changes and patch them automatically for any vulnerability without any manual intervention using Auto-Discovery and Auto Policy generation which is fastest and very quick with minimal False positives. Hence we request to ammend this clause accordingly. **Suggested Clause:-** The Vulnerability scan/Auto discovery feature should identify and patch the vulnerabilities such as xss, SQL Injection, Source code disclosure, Common web server vulnerabilities etc.		Bidder 12	As per RFP

9	83. Section WAF Page No. 106 11.3	Scan must be able to crawl the Web application	We suggest that WAF should be able to prevent the Crawlers from accessing the application. Crawlers consume resources on visited systems and often visit sites without approval. The WAF should be smart enough to sense the change automatically in backend application and patch the same without manual intervention. Hence we suggest to remove this clause. **Suggested Clause:-** Remove this clause.		Bidder 12	As per RFP
10	83. Section WAF Page No. 106 11.5	Should support scheduled scanning	The scanning should be an Ongoing process without manual intervention. Scheduling a scan can lead to Application compromise as nobody knows when an attack will be launched towards the web application. So it is suggested to place the WAF with discovery module on and continously monitoring every possbile change in application behaviour and block the attack traffic once identified as vulnerable. **Suggested Clause:-** Should support Continuous monitorin		Bidder 12	As per RFP

			g/scanning.			
11	83. Section WAF Page No. 106 11.6	Should support exclusions in scanning by the administrator	The scanning should be an Ongoing process without manual intervention. Scheduling a scan can lead to Application compromise as nobody knows when an attack will be launched towards the web application. So it is suggested to place the WAF with discovery module on and continously monitoring every possbile change in application behaviour and block the attack traffic once identified as vulnerable. **Suggested Clause:-** Should support Continuous monitoring/manual scanning.		Bidder 12	As per RFP

12	New Clause Request	The system should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, and acceleration resources to provide complete separate environment from applications and management perspective.	**Suggested Clause :** Should be appliance based solution with purpose built hardware for high performance with ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) OS The proposed device should support upto 32 Virtual Instance		Bidder 12	As per RFP
13	New Clause Request	Include industry standard certification and references.	**Suggested Clause:** OEM should be present in Gartner Magic quadrant in the latest WAF report		Bidder 12	As per RFP
14	New Clause Request	The Web Application firewall should be able to integrate with Proposed DDoS solution at Perimeter so it can share the attack details using Messaging mechanism with DDoS Mitigation appliance at the perimeter to block the attack at perimeter and prevent it from entering the DC itself.	**Suggested Clause:-** The Web Application Firewall should be able integrate with proposed DDoS Mitigation Appliance at perimeter so it can share the attack details using Messaging mechanism with DDoS Mitigation appliance at the perimeter to block the attack at perim		Bidder 12	As per RFP

			eter with DDoS Mit igator and prevent it from entering th e DC itself.			
15	84. DDoS Page No. 107 1	The proposed solution shoul d be appliance based solutio n	The DDoS mitigatio n device should be a high performance dedicated applianc e it should not hold any IP on traffic po rts. The device sho uld be invisible in t he network so that it cannot be target ed by any DDoS att ack. **Suggested Clause:-** DDoS mitigation so lution should be a dedicated applianc e (not a part of Rou ter,UTM, Applicati on Delivery Control ler,Proxy based arc hitecture or any St ateFul Device).		Bidder 12	As per RFP
16	84. DDoS Page No. 107 4	Solution must support atlea st 8X1G LAN and 8X1G WAN inerfaces	The current solutio n should be able to scale for 10 G netw ork as well conside ring future require ments in perspecti ve. For a DDoS Miti gation device whic h will placed at peri meter its highly rec ommended to go w ith SFP+ ports whic h gives the flexibilit y to adopt to 1G po rts as well as 10 G		Bidder 12	As per RFP

			ports as per the requirements. **Suggested Clause:-** Solution must support atleast 20X10G SFP+ ports.			
17	84. DDoS Page No. 107 10	System must be delivered as a rack mountable single-box solution	**Suggested Clause:** The Proposed DDoS Mitigation device should have 1U/2U form factor		Bidder 12	Remove
18	84. DDoS Page No. 107 14	Latency should be lower than 50 microseconds	Latency Factor vary from Packet size i.e. Higher the Packet Size; lesser the Latency. Majority of the Leading DDOS OEM's don't publish the Internal Testing reports wrt Latency viz-a-viz Packet Size. Exisiting clause is ambiguous, hence kindly delete or generalise this clause. **Suggested Clause:-** Latency should be lower than 100 microseconds		Bidder 12	As per RFP
19	New Clause Request	Pre-Qualification criteria must be specified to ensure quality OEM's.	OEM should be present in the Leader's quadrant for the latest Published Forrester Report for DDoS Mitigation Solution.		Bidder 12	As per RFP

			Suggested Clause:- OEM should be present in the Leader's quadrant for the latest Published Forrester Report for DDoS Mitigation Solution.			
20	New Clause Request	The DDoS Mitigation Solution should be able to integrate with Proposed WAF solution to provide precise mitigation under multivector Attack scenerio	**Suggested Clause:-** The DDoS Mitigation Appliance should be able integrate with Proposed WAF solution.		Bidder 12	As per RFP
21	85. Load Balancer Page No.110 1.6	Appliance should provide full ipv6 support and OEM should be IPv6.org gold-certified. OEM should be listed vendor for ipv6 phase-2 certification	Only Industry standard certification should be considered. Hence we suggest to ammend this clause. **Suggested Clause:-** Appliance should provide full ipv6 support.OEM should be listed vendor for ipv6 phase-2 certification		Bidder 12	As per RFP
22	New Clause Request	Pre-Qualification criteria must be specified to ensure quality OEM's.	**Suggested Clause:** OEM should be present in Gartner's LEADER magic quadrant in the latest ADC report		Bidder 12	As per RFP

23	New Clause Request	The device should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, and acceleration resources to provide complete separate environment from applications and management perspective.	**Suggested Clause :** Should be appliance based solution with purpose built hardware for high performance with ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Each virtual ADC instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) OS The proposed device should support 5 vADC from day 1 scalable to 20 vADC on the same hardware.		Bidder 12	As per RFP
1	62.1.1 Form 8C	authorized partner in India for at least last 5 years of all IT assets/offered components in proposed BOM	Kindly remove 5 years authorized partner clause.		Bidder 1	Please refer to corrigendum point 11
2	General	PBG	kindly confirm how many PBG is required to get 100%payment.		Bidder 1	Please refer to corrigendum point 4
3	General	As per application architecture diagram on page 85 0f RFP it is depicted that RDBMS used in application is MS SQL Server. But the OS of DB servers is asked RHEL. Please Clarify.			Bidder 1	The DB is My-SQL
4	General	All the servers will be deployed in same network zone (			Bidder 1	Please refer to corrigendu

		No DMZ Zone). Please clarify.				m point 15
5	General	Data will be replicated from DC to DR through storage replication only. Please Clarify.			Bidder 1	Yes
6	General	As data need to be replicated from DC to DR, Please clarify the estimated data size to be replicated and the Link bandwidth from DC to DR.			Bidder 1	The link will be provided by NIC
7	General	Price Bid	Kindly make it simple ex. Total cost for 3 years.		Bidder 1	As per RFP
8	The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats must not be signature based.	The solution must employ an on premise/cloud analysis engine using virtual execution to detect zero day and unknown threats must not be signature based.	How On Premise solution without any cloud based threat analysis can mitigate Zero Day attack, so request to add Cloud option as well		Bidder 13	As per RFP
9	The proposed solution should perform dynamic real time analysis of advanced malware to confirm true zero-day and targeted attacks. No files should be sent to third party systems or cloud infrastructure system for analysis or detection of malware	The proposed solution should perform dynamic real time analysis of advanced malware to confirm true zero-day and targeted attacks.	Please remove "No file should be sent to third party systems or		Bidder 13	As per RFP
			cloud infrastructure system for analysis and detection of Malware"		Bidder 13	As per RFP
			IPS Throughput is less than IPSec thro		Bidder 13	As per RFP

			ughput, need clarification ?			
			need the clarification on SSL and IPSec VPN as both are same but ask for different throughput		Bidder 13	As per RFP
			Change to OR on Virtual Firewall / Security Zone / Vlan		Bidder 13	As per RFP
			If device support Virtual firewall then need minimum 5 licenses		Bidder 13	As per RFP
			ICSA certification or equivalent certification		Bidder 13	As per RFP
			Server 1			
1			1. The RFP mentions 2* 8 Core CPU @ > 2.5 GHz clock speed. Pls note that we have limited processors available from Intel in the latest generation of servers launched. Hence kindly modify the clause to read as “Minimum of 2x8 Core CPU, clock speed of 2.1 GHz or higher, latest generation intel processor”		Bidder 14	Please refer to corrigendum point 7 & 8
2			2. The clause No. 1 of the RFP mentions 4x 10G base T. Plase amend the clause to read as “ 4x 10G Base T/ 2x 20G or higher Ethernet Adaptor. This will ensure maximum participation all leading OEMs of servers		Bidder 14	Please refer to corrigendum point 7& 8

			.			
3			3. Free PCI slots for expansion – This clause needs to be removed since there are limited no. of PCI slots within a Blade architecture and the same would be filled-in as per RFP reqt.		Bidder 14	As per RFP
4			4. The RFP asks for 24 DIMM slots while the actual reqt is only 32 GB Memory which can be catered to with 2* 16 GB memory modules. Hence kindly modify the clause to ask for minimum of 16 DIMM slots or more.		Bidder 14	As per RFP
5			5. The RFP mentions “Should be configured with 20 Gb connectivity per server with a minimum of 2 ports” which implies that 2 nos. of 10G ports (Fibre) on 1 no. of Ethernet Card needs to be provided. Pls clarify whether our understanding is correct. Note that in our latest Blade architecture, we cannot offer Base T as connectivity while we can only offer Fibre connectivity which is f		Bidder 14	As per RFP

			aster and newer te chnology. In case 4 * 10G Fibre needs t o be provided, the n we can offer 2 Et hernet cards which have dual ports eac h of 10G which will suffice your reqt. B ut note that in this scenario, no free sl ot will be available in the Blade server . Kindly clarify to e nsure that maximu m participation is made from all leadi ng OEMs.			
6			6. The RFP mention s “Blade chassis sh all be 19" Electroni c Industries Allianc e Standard Width r ack mountable and provide appropriat e rack mount kit”. Kindly note that we will be providing th e Blade Chassis whi ch will be “Modula r Chassis Infrastruc ture” which is com patible to 19” Rack. Hope this is OK oth erwise pls clarify w hat is meant by 19" Electronic Industrie s Alliance standard s.		Bidder 14	As per RFP
7			Server 2		Bidder 14	

8			1. The RFP mentions 2* 12 Core > 3.0 GHz CPU clock speed. Pls note that Intel has a processor matching the Cores as 12 Cores which is = 3.0 GHz but not more than 3 GHz clock speed. Kindly modify the same to read as “Minimum of 2x12 Core CPU, clock speed of 3.0 GHz or higher, latest generation intel processor”		Bidder 14	Please refer to corrigendum point 8
9			2. The clause No. 1 of the RFP mentions 4x 10G base T. Please amend the clause to read as “ 4x 10G Base T/ 2x 20G or higher Ethernet Adaptor. This will ensure maximum participation all leading OEMs of servers.		Bidder 14	Please refer to corrigendum point 8
10			3. Free PCI slots for expansion – This clause needs to be removed since there are limited no. of PCI slots within a Blade architecture and the same would be filled-in as per RFP reqt.		Bidder 14	As per RFP
11			4. The RFP asks for 24 DIMM slots while the actual reqt is only 256 GB Memory which can be catered to with 4* 64 GB OR 8* 32 GB memory modules. He		Bidder 14	As per RFP

			nce kindly modify t he clause to ask for minimum of 16 DI MM slots or more.			
12			5. The RFP mention s “Should be config ured with 20 Gb co nnectivity per serv er with a minimum of 2 ports” which i mplies that 2 nos. of 10G ports (Fibre) on 1 no. of Etherne t Card needs to be provided. Pls clarify whether our under standing is correct. Note that in our lat est Blade architect ure, we cannot off er Base T as connec tivity while we can only offer Fibre con nectivity which is f aster and newer te chnology. In case 4 * 10G Fibre needs t o be provided, the n we can offer 2 Et hernet cards which have dual ports eac h of 10G which will suffice your reqt. B ut note that in this scenario, no free sl ot will be available in the Blade server . Kindly clarify to e nsure that maximu m participation is made from all leadi ng OEMs.		Bidder 14	As per RFP

13			6. The RFP mentions “Blade chassis shall be 19" Electronic Industries Alliance Standard Width rack mountable and provide appropriate rack mount kit”. Kindly note that we will be providing the Blade Chassis which will be “Modular Chassis Infrastructure” which is compatible to 19” Rack. Hope this is OK otherwise pls clarify what is meant by 19" Electronic Industries Alliance standards.		Bidder 14	Understanding is correct
14		CACHE : 4GB Controller cache with 72 hours battery backup	CACHE : 32 GB Controller cache with 72 hours battery backup or cache de stage to SSD or equivalent technology to protect cache data in event of power failure	Storage to deliver 150,000 IOPS, controller cache minimum should be 32GB	Bidder 14	Please refer to corrigendum point 5
15		DRIVE INTERFACE : 4 drive ports—Fiber Channel (FC) Switched and FC Arbitrated Loop (FC-AL) standard, auto-sensing 1Gbps/2 Gbps/4 Gbps	DRIVE INTERFACE : 4 drive ports—SAS/ Fiber Channel (FC) Switched/FC Arbitrated Loop (FC-AL) standard, auto-sensing 3Gbps/6 Gbps/12 Gbps	As per current technology all vendors have SAS 12/6Gbps as drive interface	Bidder 14	As per RFP
16		HOST PORT : 4 no Switched FC or FC-AL/4 Gb/sec, 2 Gb/sec, 4 Gb/sec	HOST PORT : 4 no Switched FC or FC-AL/4 Gb/sec, 2 Gb/sec, 4 Gb/sec or Higher	As per current technology all vendors have FC 16Gbps as front end interface	Bidder 14	As per RFP

17		WAN Replication capability		Need Clarity does replication ports and license are required now ? replication ports 10G BaseT or 10G SFP+ depends up on customer existing LAN Switch type/ ports.	Bidder 14	As per RFP