No. 17/20/2018-PMMVY Part (1)
Government of India
Ministry of Women and Child Development
PMMVY Section
*****

Shastri Bhawan, New Delhi-1
Dated: 5th October 2018

CORRIGENDUM

Subject: Issue of corrigendum with respect to the Request for Proposal (RFP) for Supply, installation and maintenance of IT infrastructure for hosting PMMVY-CAS.

The undersigned is directed to refer to RFP- No. 17/20/2018-PMMVY, with respect to RFP for Supply, installation and maintenance of IT infrastructure for hosting PMMVY-CAS issued on Ministry's website as well as on CPP Portal and issue the corrigendum as **Annexed.**

05/10/18

(V.C. Choudhary)
Under Secretary to Government of India
Tel. NO.:011-23388513
Email: vc.choudhary@nic.in

Corrigendum

REQUEST FOR PROPOSAL (RFP) for Supply, Installation and Maintenance of IT Infrastructure for PMMVY-CAS

*****

Sl. No.	RFP Section/ sub-section	Page No.	Relevant clause of RFP	Modified Clause
1.	35 , Table Sl. No. 3	44	The Bidder should have a minimum turnover of Rs. 100 crores per annum during last three financial years in India (FY 2013-14, 2014-15, 2015-16)	The Bidder should have a minimum turnover of Rs. 100 crores per annum during last three financial years in India (FY 2014-15, 2015-16, 2016-17)
2.	36, Table Sl. No-C1	66	The bidder should have experience in executing similar projects (procuring, supplying, commissioning and supporting servers/ storage) in Government/ PSU sector in India with order value more than INR 10 crore"	The bidder should have experience in executing similar projects (procuring, supplying, commissioning and supporting servers/ storage) in Government/ PSU sector/ Banks/ BFSI in India with order value more than INR 10 crore"
3	Additional Clause Number 1			Load balancer specs mentioned in Annexure-1
4	Additional Clause number 2			Sandbox /Anti-APT specs mentioned in Annexure-1
5	Clause No-9	25	Hardware/ System Software delivery report (mapping with BOM): 1 month from Project initiation Commissioning Report and Go-Live Report (with applications migrated to new setup) : 3 months from Project Initiation	Hardware/ System Software delivery report (mapping with BOM): 2 month from Project initiation Commissioning Report and Go-Live Report (with applications migrated to new setup) : 4 months from Project Initiation
6	Clause No-C2	67	The bidder should have experience in procuring, supplying and commissioning the proposed infrastructure of proposed OEM	The bidder should have experience in procuring, supplying and commissioning the proposed infrastructure.

7	Section 83 - WAF, Clause no. 2.4	115	Should deliver at least 3 Gbps of WAF (HTTPs) throughput	Should deliver at least 1 Gbps of WAF (HTTPs) throughput
8	Payment Schedule	27	60% of the cost would be payable on delivery of the hardware , 20% of the delivered hardware cost would be payable on successful installation of the hardware/ System Software , 10% of the cost will be payable post-go-live after complete PMMVY-CAS setup is migrated to new infrastructure , 1.25% of payment would be payable at the end of each quarter for 8 quarters across a period of 24 months	70% of the cost would be payable on delivery of the hardware , 10% of the delivered hardware cost would be payable on successful installation of the hardware/ System Software , 10% of the cost will be payable post-go-live after complete PMMVY-CAS setup is migrated to new infrastructure , 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.
9	50	57	Personal information of the beneficiaries of DBT schemes of the Ministry, including their name, date of birth, Aadhaar number, mobile number, bank account number, etc.	File Integrity tool included for protecting Personal Information from insider Threat.
10	79 Enterprise Management System	108	1.8 Support for backup and storage	clause removed ~~1.8 Support for backup and storage~~
11	75 Server 1-Processor	104	Minimum of 2x8 Core CPU, clock speed > 2.5GHz, latest generation intel processor , 2x600GB 15k RPM HDD , 4x10Gb 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 BaseT, 1xDP 16Gb FC HBA, RHEL, RHEL,Free PCIe Slots for expansion
12	75 Server 1-Network	104	Should be configured with 20 Gb connectivity per server with a minimum of 2 ports	Should be configured with Minimum 20 Gb connectivity per server with a minimum of 2 ports
13	Section 1, :Important Dates	6	• Last date and time for bid submission is 05.10.2018 ; 15:00 Hours • Date and time for opening of Technical bids is 05.10.2018 ; 16:00 Hours	• Last date and time for bid submission is 15.10.2018 ; 11:00 Hours • Date and time for opening of Technical bids is 15.10.2018 ; 13:00 Hours

14	6.1.1: Bill of material	12	<table><tr><th>Type of Infrastructure</th><th>DC (qty)</th><th>DR (qty)</th></tr><tr><td>WebServer (Server 1)</td><td>2</td><td>2</td></tr></table>	<table><tr><th>Type of Infrastructure</th><th>DC (qty)</th><th>DR (qty)</th></tr><tr><td>WebServer (Server 1)</td><td>5</td><td>5</td></tr></table>
15	6.1.1: Bill of material	14	Server 2 (Training server is used for creating a training environment for various stakeholders and whenever there is a change in software. Training data, which is dummy data, cannot be allowed to be uploaded on production environment and interfere with the live financial environment. This server shall contain the multiple instances of training data for nationwide trainings of users.)	Server 2 ~~(Training server is used for creating a training environment for various stakeholders and whenever there is a change in software. Training data, which is dummy data, cannot be allowed to be uploaded on production environment and interfere with the live financial environment. This server shall contain the multiple instances of training data for nationwide trainings of users.)~~
16	77 SAN Storage- SUPPORTED DRIVES S. No. 7	106	SUPPORTED DRIVES : 300GB to 1.2 TB size / both SAS and FC drives	SUPPORTED DRIVES : 300GB to 1.2 TB size / SAS (mandatory) and FC drives(optional)
17	77 SAN Storage S. No. 6	106	“RAID LEVEL SUPPORT : 0, 1, 3, 5, 1+0”.	“RAID LEVEL SUPPORT : 0, 1, 5, 1+0”, 3(optional)
18	77 SAN Storage S. No. 10	106	OS SUPPORT : Windows 200x, HP-UX, Linux, AIX, Solaris	OS SUPPORT : Windows 20Xx, HP-UX(Optional), Linux, AIX (Optional), Solaris
19	78 SAN Switch S. No. 8	107	Ethernet, RS232 and IP over Fiber Channel	Ethernet, RS232 and IP over Fiber Channel/ RJ-45 in-band over Fiber-Channel.

20	Additional Clause Number 3	-	-	Firms registered under NSIC under Single point registration scheme are exempted from submission of EMD. But, in this respect, they should submit their valid NSIC Certificate.

Annexure-1

Load Balancer		
S.no	**Technical Specifications**	**Compliance (Yes/ No)**
1	**Hardware**	
1.1	Should be appliance based solution with purpose built hardware for high performance.	
1.2	Intel based CPU with 8 GB RAM to support multiple features and load balancing functions.	
1.3	The appliance should have minimum 8 triple speed gigabit 10/100/1000 copper ports and option for2*10G to cater future requirements.	
1.4	The appliance should have 5 Gbps of system throughput and scalable to 10 Gbps on same appliance. The appliance should support a minimum of 2500 SSL TPS (2K Keys) from Day 1	
1.5	Should provide 3M concurrent connections and scalable to 4M on same device.	
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.	
2	**Load balancing Features**	
2.1	The solution should able to load balance both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.	
2.2	The solution should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.	

2.3	The solution should support for policy nesting at layer7 and layer4. it should able to combine layer4 and layer7 policies to address the complex application integration.	
2.4	Should support Static NAT, Port based NAT and advanced NAT	
2.5	IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support.	
2.6	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..	
2.7	The solution should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers. The Appliance should also support acting as a Webagent service to implement explicit Forward proxy mode and to perform DNS Caching	
2.8	The solution should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..	
2.9	The solution must support Single Sign-On (SSO) for web based applications and web based file server access. It should also supports SAML secure application access	
2.1	The solution should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. It should support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".	

2.11	Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.	
2.12	The solution should have script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. It should support ePolicies to customize new features/rules to re-direct the traffic on specific parameters.	
3	**High Availability and Cluster**	
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 using standard VRRP.	
3.2	Stateful session failover with N+1 clustering support when deployed in HA mode	
3.3	Support for multiple communication links for real-time configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc.. and heartbeat information	
3.4	should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to speed up the failover	
3.5	should support for secondary communication link for backup purpose.	
3.6	should support floating IP address and group for stateful failover support. Appliance must have support 256 floating ip address for a floating group	

3.7	should support built in failover decision/health check conditions including, CPU overheated, system memory, process health check, unit failover, group failover and reboot	
3.8	should also have option to define customized rules for gateway health check - the administrator should able to define a rule to inspect the status of the link between the unit and a gateway	
3.9	Configuration synchronization at boot time and during run time to keep consistence configuration on both units.	
4	**Security and Application Performance**	
4.1	Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation.	
4.2	Should support TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed.	
4.3	TCP optimization option configuration must be defined on per virtual service basis not globally.	
4.4	Software based compression for HTTP based application, support and high speed HTTP processing on same appliance.	
4.5	Should support QOS for traffic prioritization, CBQ , borrow and unborrow bandwidth from queues.	
4.6	Should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols.	
4.7	Should support rate shaping for setting user defined rate limits on critical application.	
4.8	Should support integrated firewall module to protect the device itself from network based DOS and DDOS attacks.	

4.9	Appliance should have security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation.	
5	**Centralized Management**	
5.1	The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.	
5.2	Should support XML-RPC for integration with 3rd party management and monitoring of the devices.	
5.3	The appliance should provide detailed logs and graphs for real time and time based statistics	
5.4	Appliance must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback.	
5.5	The system should support led warning and system log alert for failure of any of the power and CPU issues	

APT Solution

S.no	Technical Specifications	Compliance (Yes/ No)
1	The solution should support deep packet inspection of SSL encrypted traffic (including HTTPS) for both incoming and outgoing	
2	The solution should provide detection, analysis and remediation capability against APT & SSL based APT attacks.	
3	The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and must not be signature based.	

4	The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database.	
5	The proposed solution should perform dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks. No file should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware	
6	The proposed solution should automatically detect and confirm multistage zeroday malware and targeted attacks without prior knowledge of the malware.	
7	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.	
8	The proposed solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.	
9	The solution must support pre-populated Licensed copies of Operating systems and applications/softwares (like Microsoft Office). There should be no requirement for the customer to buy additional license.	
10	The system should be able to support file sizes upto 50 mb or more	
11	The proposed solution should have the ability to analyse, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents,	

12	common multimedia contents such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zeroday attacks.	
13	The proposed solution should capture and store packet captures of traffic relevant to the analysis of detected threats.	
14	The proposed solution should have the ability to display the geo-location of the remote command and control server(s) when possible.	
15	The proposed solution should have the ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack.	
16	The proposed solution should be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, or SNMP).	
17	The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP) & inline mode	
18	The proposed solution should be capable to block inbound malicious exploits delivered via a web channel and outbound call-back communications when deployed in inline, or out-of-band mode.	
19	The proposed solution should be able to analyse email attachments and malicious links for static and dynamic analysis	
20	The proposed solution should support SMB / CIFS / NFS protocol for sharing and transferring files	
21	The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress.	

22	The solution should provide reports in (but not limited to) PDF/CSV formats.	
23	The solution should have anti-evasion capabilities to prevent malwares detection of being run/executed in the vitualized environment.	
24	The solution should support for SIEM log integration.	
25	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.	
26	Minimum number of Interfaces - 4x GE & 2 x 10G	
27	Number of VM's should be atleast 56 from day 1	
28	It should support Sandbox Analysis for multiple operating systems like WinXP,Win7,Win8,Win10	
29	The APT appliance should be able to process minimum of 1000 files/hour (either web or network or both) on the VM sandboxing	
30	High Availability & Maximum Scalability	
31	The solution should have dual AC power supply fully populated (within box) from day one	

File Integrity Monitoring Tool

S.No	Specifications	Compliance (Yes/ No)
1	The on premise application should protect digital files from Tampering	
2	It should protect data integrity and create an immutable audit trail of activities log	
3	It should have Fast monitoring at File level.	
4	The monitoring speed should be upto 500k files in 10 seconds at File level.	

5	If tampered file is detected, it must be recovered automatically within 1 min	
6	The application should have the following features:	
7	Data Protection	
8	Data Recovery	
9	Auto Recovery	
10	Manual Recovery	
11	KSI Block Chain	
12	High Speed Monitoring	
13	Alert System	
14	Role based permission	
15	Reporting	
16	The technology should work on “keyless” signature to any type of data.	
17	The signature should store with the data, as an attribute which can be used to verify the time of creation, identity of creator and integrity of the data, independently from insiders, keys, secrets and certificates, and without the data leaving the premises.	
18	This Technology must have implemented atleast in two places anywhere in the world and proof should be submitted like Purchase order copy or Project completion letter from the end customer	