Corrigendum No. 1 Tender Document for IT Infrastructure for Tripura State Data Center at Agartala					
S. No.	**RFP page no. and Point No**	**Clause Title**	**Queries/Clarification Sought**	**Justification by Bidder with required Changes**	**Remarks**
1	(Page no 63 of 100) 9	NIPS: Network Intrusion Protection System	Latency must be < 60 microseconds. must support at least 30,000,000 concurrent connections	The clause asks for Latency <60 microsoeconds and minimum concurrent connections 30,000,000. The figures asked for latency and concurrent connection is very less and may hamper the performance of NIPS considering the throughput of 80 gbps asked. Hence request you to change the clause tp make NIPS more performance centric and claue should read as "**Latency must be 40 microseconds. must support at least 100,000,000 concurrent connections**"	no change , as per RFP
2	(Page no 64 of 100) 18	NIPS: Network Intrusion Protection System	The device must have the ability to identify/block individual applications (e.g. Facebook or skype) running on one protocol (e.g. HTTP or HTTPs)	The clause asks for NIPS to block individual applications but NIPS works on detection and blocking of network packets not file.This ask is for Proxy not for NIPS.Hence request you to change the clause as below "**The device must have the ability to identify/block malicious applications traffic running on one protocol (e.g. HTTP or HTTPs)**"	no change , as per RFP

3	(Page no 64 of 100) 15	NIPS: Network Intrusion Protection System	The device must provide advanced DOS/DDOS protection and not just signatures based employing a combination of threshold-based and selflearning, profile-based detection techniques, volume based and exploits signatures to detect DoS and DDoS attacks	The cluase asks for NIPS device must prevent DOS/DDOS attacks through Signature based filters, Zero day Filters and Self Learning Filters. The self learning capability in NIPS favors a specific OEM only and has performance implications in the Network. Hence request you to make the ask generic and change the clause as "**The device must provide advanced DOS/DDOS protection through signatures based, profile-based detection techniques and Zero day Filters and exploits signatures to detect DoS and DDoS attacks**"	no change , as per RFP
4	(Page no 64 of 100) 19	NIPS: Network Intrusion Protection System	The device must prevent SSL protocol-based attacks	The clause asks for prevention of SSL protocol based attacks but with no mention of minimu of SSL Inspection throughput requirement. Hence request you to change the clause incorporating SSL Traffic InspectionThroughput requirement "**The device must prevent SSL protocol-based attacks with minimum 5 gbps SSL Inspection throughput, supported SSL connection per second 7K, SSL Concurrent connections 1 Lakh** "	no change , as per RFP

5	(Page no 65 of 100) 27	NIPS: Network Intrusion Protection System	The device must have the feature of Self-learning profile-based detection/ Network Behaviour Analysis	The clause asks for Network Behavior Analysis (NBA) in NIPS. The major task of NIPS is to block threats on the basis of vulnerabilities and not NBA. This ask favors a specific OEM only. Hence request you to make the ask generic and change the clause as "**Ths NIPS Solution must have the feature of profile-based & vulnerability threat detection & prevention capabilities"**	no change , as per RFP
6	(Page no 65 of 100) 35	NIPS: Network Intrusion Protection System	The IPS solution offered must be rated as ‘leaders’ or 'Challengers' in the latest Magic Quadrant by Gartner	The clause asks for NIPS solution to be either Leader or Challenger in Gartner Magic Quadrant. Including Vendors who are Challengers in the bid participation will end up compromising the detection/prevention quality with performance degradation.Hence request you to change the clause as follows " **The IPS solution offered must be rated as ‘leaders’ in the latest Magic Quadrant by Gartner**"	no change , as per RFP
7	(Page no 81 of 100) Under "Schedule of Requirement"	Point 4 - License(2.3.2 Host Intrusion Prevention System)	No technical specification asked for Host Intrusion Prevention System	Sir the clause asks for host Intrusion Prevention System without any technical specifications. This will lead to no clarity of the solution w.r.t. quality and performance. Hence rqeuest you to incorporate minimum technical specifications for vendor participation shared in this sheet.	Added below in the corrigendum

8	(Page no 81 of 100) Under "Schedule of Requirement"	Point 4 - License(2.5.3 Antivirus Management Server , 2.5.4 Antivirus Endpoint Licenses)	No technical specification asked for Antivirus Mangement Server and Endpoints. Hence incorporate this technical specification.	Sir the clause asks for Antivirus Management Server without any technical specifications. This will lead to no clarity of the solution w.r.t. quality and performance. Hence rqeuest you to incorporate minimum technical specifications for vendor participation shared in this sheet.	Added below in the corrigendum
S. No.	**Host Intrusion Protection System**				**Compliance (Yes / No)**
1.1	The HIPS shall protect against the entire classes of attacks, including port scans, buffer overflows, Trojan horses, malformed packets, malicious HTML requests, and e-mail worms.				
1.2	The HIPS solution should automated, real-time intrusion detection and should protect by analyzing the events, operating system logs and inbound/outbound network traffic on enterprise servers.				
1.3	The HIPS solution should offer an enterprise-scalable architecture; the HIPS should be scalable to thousands of agents per manager.				
1.4	The solution should provide protection for Web Servers, Applications and Database Servers				
1.5	The HIPS solution should provide for Server Protections with ability to Filter HTTP requests to prevent directory traversal, Unicode, and denial-of-service (DoS) attacks and also protect against SQL/MYSQL/MSSQL injection attacks & cross-site scripting (XSS) attacks				
1.6	The HIPS solution should provide Executable matching for applications based on path, hash, digital signature and file description for signatures and exception and not just on path basis.				
1.7	The HIPS solution should use the HTTP and SSL protocols for the management interface and for the communication between the HIPS and management center.				
S. No.	**Antivirus Solution**				**Compliance (Yes / No)**
1	Antivirus Software. The key features for antivirus for endpoints shall be as follows:-				
1.1	The Antivirus solution should support automatic centralized pattern updating and distribution				
1.2	The Antivirus solution should support restriction to un-installation of antivirus solution by users.				

1.3	The Antivirus solution should support Folder and file type scan exclusions for performance enhancement	
1.4	The Antivirus solution should support file scan caching to avoid repetitive scanning of files which are unchanged since the previous scan	
1.5	The Antivirus solution should automatically scan all storage devices (Internal & External) not limited to Floppy disks, Compact disks, USB devices and Network shares in real-time when accessed.	
1.6	The Antivirus solution should provide multiple policies to lockdown the server like – change in registry, Web Browser file settings, Exe file execution etc to block unknown zero day attacks and reduce dependency on frequent signatures	
1.7	The Antivirus solution should be capable of detecting and preventing buffer overflow vulnerability, irrespective of the exploit that is using the buffer overflow vulnerability.	
1.8	The Antivirus solution should be capable of blocking TCP/IP ports on the System and also creating exceptions for specified applications to use these blocked ports.	
1.9	Discover and Report the IP Address of the end-point system (infection source) that sent malicious code to the server and optionally, block further communications from the infection source end-point system for a configurable time period or indefinitely.	
1.10	The Antivirus solution should provide Self-protection from modifying or disabling Antivirus Client.	
1.11	The Antivirus solution should scan system memory for installed rootkits, hidden processes, and other behavior that suggests malicious code is attempting to hide itself.	
1.12	Proposed solution should allow configuring different policies for different set of Processes.	
1.13	The Antivirus should allow for automated/ manual rollback of virus definition, if required.	
1.14	The Antivirus should be able to lock down all anti-virus configurations at the servers.	
1.15	The Antivirus should be capable of detecting and blocking communication from hosts that are spreading viruses/worms.	
S. No.	**Antivirus Management Server**	**Compliance (Yes / No)**
2	Centralized AV management server should support the following:-	

2.1	Should provide with On -Premised centralized management with policies to update the Database / Threat intelligace via Real - time updates via Web . the clients can be centrally managed/configured for antivirus masnagement server	
2.2	To be able to centrally download updates for AV software and deploy updates automatically to the antivirus environment.	
2.3	The server component should have an option to do a manual and a scheduled update.	
2.4	Have ability to take action from the centralized console including issuing commands to antivirus clients and getting immediate responses.	
2.5	Have ability to apply appropriate settings to AV client from a centralized console.	
2.6	Have ability to collect logs from all AV clients and provide information through log queries or reports.	
2.7	Have ability to notify the administrator from a centralized location.	
2.8	Provide sort and search function on the client tree in the management console to sort the clients in the required order and search for a specific client	
2.9	Have the ability to control network access based on a endpoint's compliance with organization's antivirus health policy, remediate the non-compliance to health or restrict its access to network resources.	
2.1	Shall manage the antivirus programs on the network from a single pannel console.	
2.11	Shall provide network wide virus statistics and analysis.	
2.12	Shall support leading web browsers.	
2.13	It shall be able to monitor remote locations over WAN links for antivirus activity.	
2.14	Shall offer a hierarchical structure for job delegation so administrators can determine access control.	
2.15	Have the ability to classify the management system's users into Administrator, Power User or Operator roles.	
2.16	It should support central deployment of Outbreak Prevention Policies to all the managed antivirus products.	
2.17	Shall be able to have different operator assigned separate access to Individual location for job delegation and separation of task and responsibility.	
2.18	Shall utilize secure communications between Management Server and managed product(s).	

2.19	Have the ability to run a clean-up scan on all the clients from a single console without user intervention.	
2.2	Have the ability to deploy the updates manually to all the clients with an update now option	
2.21	Control Client access to the antivirus program installed by giving restricted access to the program folder and registry files thereby preventing the user from deleting and altering the files necessary for the client program to run properly.	
2.22	Should have an option to roll-back the pattern file and scan engine.	
2.23	Support multiple remote installations.	
2.24	**Notification/Logging**	
2.24.1	Customizable client alert message for virus detection.	
2.24.2	Notification through E-mail ,POP-UP , SNMP trap or through Windows Event Log.	
2.24.3	Generate Virus activity log, update log, Personal firewall/intrusion detection log.	
2.24.4	Client connection status log and Server system event log.	
2.24.5	Notify the administrator in case of License Violation.	
2.24.6	Send notification to the infection source.	